Theory

Chapter 1 (This chapter is blank in HDS version) ····· THEO 01-0000
Chapter 2 Overview of the Subsystem ····· THEO 02-0000
Chapter 3 Description of Operations ····· THEO 03-0000
Chapter 4 Maintenance Actions ····· THEO 04-0000
Chapter 5 LAN Configuration Settings ····· THEO 05-0000

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

Chapter 1 (This chapter is blank in HDS version)

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

Chapter 2 Overview of the Subsystem

This chapter provides an overview of the Hitachi Data Ingestor (HDI), Hitachi Content Platform (HCP) subsystems.

Table 2-1 describes the terms used in this manual.

Table 2-1 Definition of Terms (1/2)

No.	Term	Meaning
1	HCP	Abbreviation of Hitachi Content Platform. The HCP is a system for long-term data storage and management. The data of the file system created by HDI can be migrated to HCP.
2	Namespace	A namespace that can be created in HCP. The namespace is a logical group, and an object stored in one namespace cannot be referred to from another namespaces. It specifies one namespace per file system of HDI.
3	Tenant	One grouped a namespace that can be created in HCP. One tenant can own multiple namespaces. One tenant is allocated to one HDI for migration.
4	Migration	A function to copy the file data on HDI to HCP.
5	Recall/ Entire recall	A function to read the substantial data of the file from HCP in response to the HDI client access that HDI client Read/Write the stub file.
6	Stub file	A file that file property is remained, but that data on HDI moved to HCP. About the file on HDI, the data of the file are duplicated to HCP by Migration, but after that the file on HDI become unsubstantial because HDI stub data and remained only property. If a client require to Read /Write stub file, HDI respond it using Recall function that read out the substantial data of the file from HCP.
7	Retention	A function to prevent a file from changing during a specified period.
8	WORM	Abbreviation of Write Once Read Many. A WORM file is a read only file. Once a file is converted to a WORM file, it cannot be writable again because not only the data but also the metadata are prohibited from being changed.
9	HFSM	Abbreviation of Hitachi File Services Manager. HFSM is a program required for the system administrator to manage the HDI by using a GUI in the cluster configuration, and must be installed on a management server. HFSM is also used for setting migration policies.
10	Management GUI	Management GUI is an interface used by the system administrator to manage the HDI by in the single node configuration. Management GUI is also used for setting migration policies.
11	Migration policy	Setting of HCP (tenant, namespace) of the migration destination, file types that can be the migration target and a schedule to execute the migration. HDI executes the migration according to the migration policy.
12	node	A server to receive the request of Read/Write using CIFS/NFS. HDI consist of two servers in cluster configuration, and HDI consist of one server in single node configuration. Data is stored in connected disk array in the case of cluster configuration, and data is stored in the connected disk array or internal drives within the server in the case of single node configuration.
13	BMC	Baseboard Management Controller. This is a controller tip to be installed in a server, and monitors hardware status separately from the main processor or the peripheral tip set.
14	front-end LAN	LAN which the client uses for accessing data
15	Management LAN	LAN which the system administrator uses for operating and maintaining HDI

Copyright © 2010, 2016, Hitachi, Ltd.

Table 2-1 Definition of Terms (2/2)

No.	Term	Meaning
16	Private Maintenance LAN	LAN which the maintenance personnel use for maintaining HDI
17	IP-SW	Layer 2 Switch
18	FC-SW	Fibre Channel Switch
19	Virtual Server	HDI does not support. Virtual server which runs in node. Receives Read/Write requests like node. Unlike node, it is possible to run multiple Virtual Servers because they have no physical substance.
20	BMC direct connection configuration	A cluster configuration in which the BMC port to connect to the reset port of the other side node. To reset the opposite side of the node, execute without going through IP-SW.
21	BMC and management SW connection configuration	A cluster configuration in which the BMC port to connect to the management LAN IP-SW. To reset the opposite side of the node, execute through IP-SW.
24	Configuration of the single node with spare for Cloud	Configuration to build the Active Standby system by connecting multiple HCP linked single nodes to the same network. Operating node is called “Active node” and a backup node is called “Standby node”.
25	HCP-AW	Abbreviation of Hitachi Content Platform Anywhere. It is a system which is shared by accessing to data from various locations. If a user adds data to HCP-AW, that data is saved in HCP and the data is shared through user terminals (computer, smart phone, tablet computer etc.) HCP-AW administrator builds and monitors several nodes in remote. HCP-AW administrator configures, monitors and manages the system using the Web application called the management console.
26	flash drive	A data drive that uses a solid-state memory device instead of a rotating hard disk.
27	FMD (Flash Module Drive)/ FMC (Flash Module Compression)	FMD/FMC are a high speed data storage device that includes a custom flash controller and several flash memory sub-modules on a single PCB.FMC is supported accelerated compression function.
28	Active File Migration	Before migration starts, the data of the specified files is copied to the work space created for each file system. Because the data copied to the work space is migrated to the HCP system, files can be modified during the migration without affecting the processing. This work space is written “the work space for AFM” on this manual. And it is same to mean “the work space” on administrator’s documents.
29	large file transfer	A large file is divided and migrated multiple times. When using this function, only the portion of the target file that is updated from the last migration is migrated.

Copyright © 2011, 2017, Hitachi, Ltd.

2.1 Basic Specifications of the Subsystem

HDI is a system where two nodes, a management LAN IP-SW, a disk array subsystem, and an FC-SW are combined in the cluster configuration, and a system of one node and, in some cases, a disk array subsystem are combined in the single node configuration.
This section shows an overview of the disk array subsystem of the node used in HDI.
Refer to the manual of each of the devices for the overview of the other devices than the nodes.

(1) Specifications of disk array subsystem
For details about the subsystem specifications for the HDI nodes and the names and locations of the respective parts of the nodes, refer to the manuals provided by the respective hardware vendors.

Copyright © 2010, 2012, Hitachi, Ltd.

2.2 Overview of the Connection

As for the system configuration, there are three types of node configuration of different usages, which are the Basic Configuration, the HDI for HCP configuration, and the HDI for Cloud configuration. The figures showing the overview are respectively shown below.

(1) Basic Configuration
Basic Configuration is the configuration which is not linked up with HCP.
HDI does not support Basic Configuration.

Copyright © 2010, 2012, Hitachi, Ltd.

(2) The configuration of HDI for HCP

(2-1) The configuration of HDI for HCP in the cluster configuration

Figure 2.2-1 shows the overview of connection diagram in the configuration of HDI for HCP.
As shown in the figure, the HDI and HCP work together while sharing the disk array subsystem.
Refer to "Installation '1.1.4 Overall configuration diagram (2) Overall system configuration diagram in the configuration of HDI for HCP' (INST 01-0073)" for the entire system configuration figure, and refer to "A.2.3 LAN Cable" for the details of cable connection.
Note that the dotted line part and the dashed line part in the figure show system ranges.

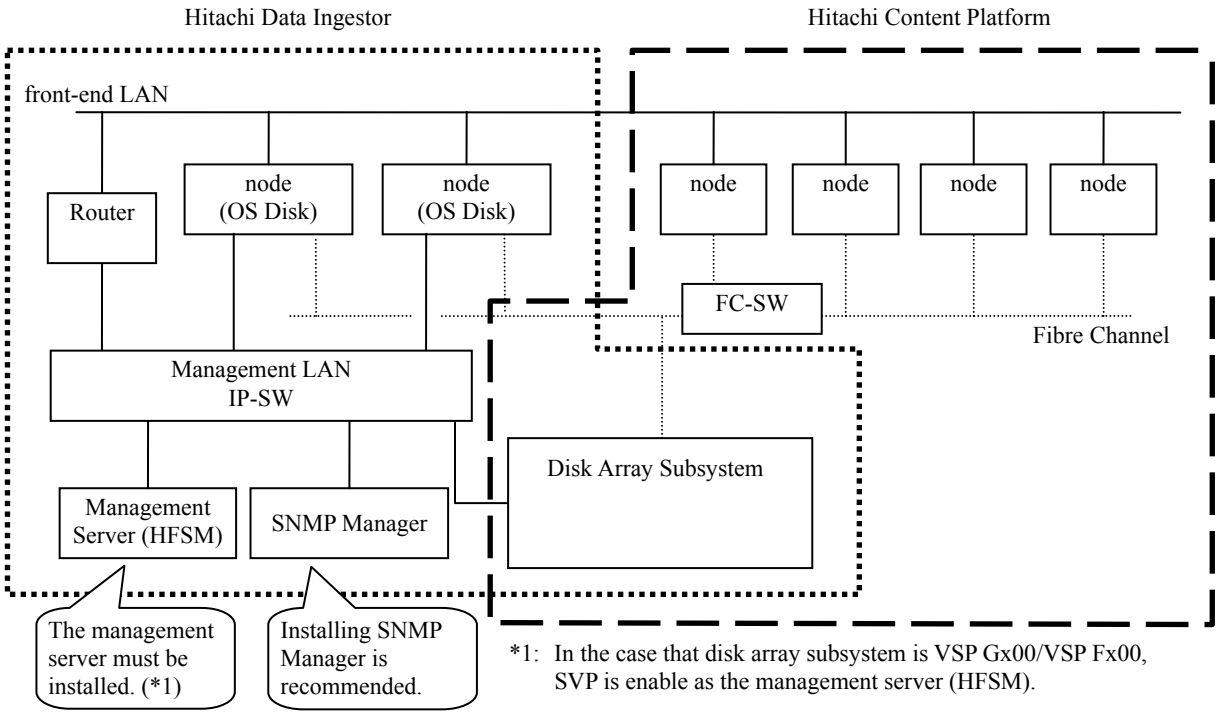


Figure 2.2-1 Overview of Connection Diagram in the Configuration of HDI for HCP (In the cluster configuration)

Copyright © 2010, 2016, Hitachi, Ltd.

(2-2) The configuration of HDI for HCP in the single node configuration
Figure 2.2-2 shows the overview of connection diagram in the configuration of HDI for HCP in the single node configuration. Note that the dotted line part and the dashed line part in the figure show system ranges.

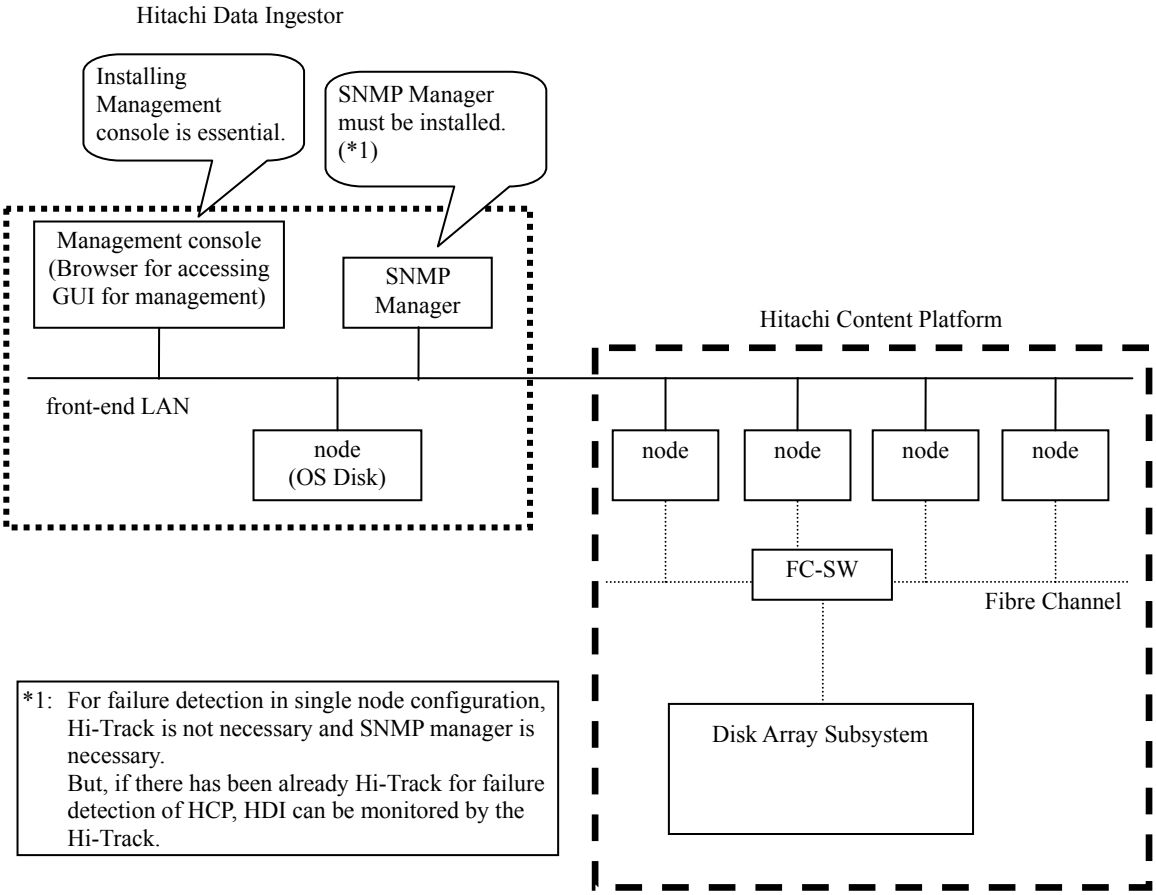


Figure 2.2-2 Overview of Connection Diagram in the Configuration of HDI for HCP (In the single node configuration)

Copyright © 2011, Hitachi, Ltd.

(3) The configuration of HDI for Cloud

(3-1) The configuration of HDI for cloud in the cluster configuration

Figure 2.2-3 shows the overview of connection diagram in the configuration of HDI for Cloud in the cluster configuration (BMC and Management SW connection configuration).

Figure 2.2-4 shows the overview of connection diagram in the configuration of HDI for Cloud in the cluster configuration (BMC direct connection configuration).

The functions are linked via WAN on the HDI and the HCP side.

Note that the DNS server on the HDI side needs to set a forwarder for the DNS server on the HCP side. By setting the forwarder, even if the failover is done on the node of HCP due to a failure, the communication to HCP can be resumed as soon as the DNS server is updated.

The site on the HCP side must be the HCP-alone configuration, not the configuration of HDI for HCP.

Refer to "Installation '1.1.4 Overall configuration diagram (3) Overall system configuration diagram in the configuration of HDI for Cloud (cluster node)' (INST 01-0077)" for the entire system configuration figure, and refer to "A.2.3 LAN Cable" for the details of cable connection.

Note that, the dotted parts and the dashed parts in the figure show system ranges.

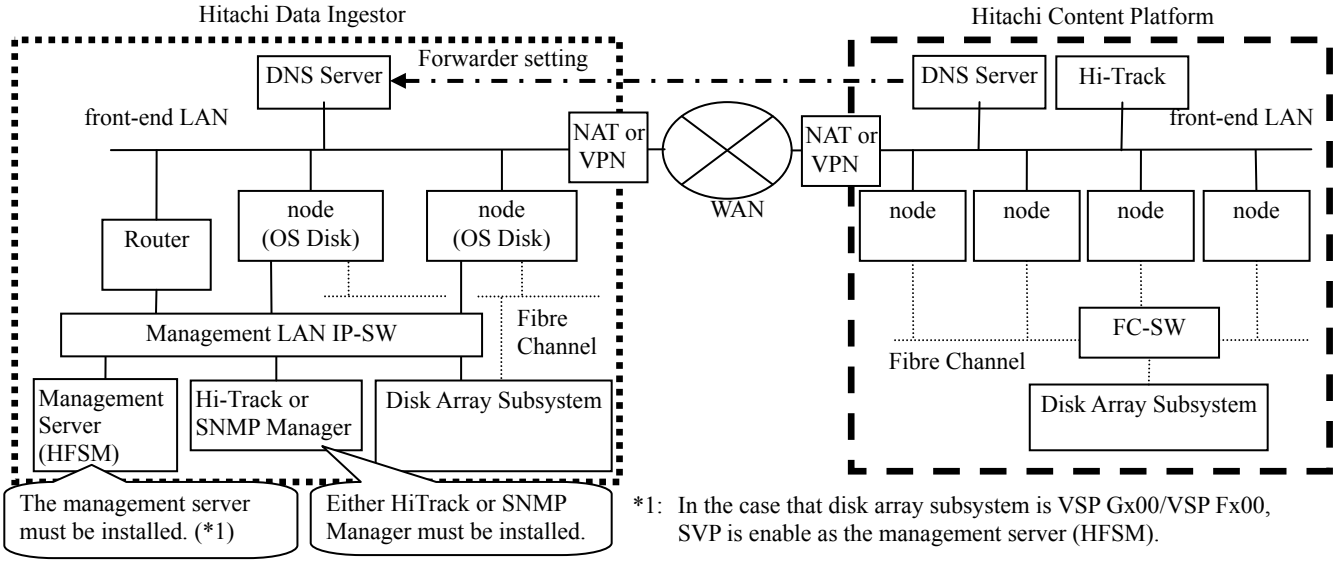


Figure 2.2-3 Overview of Connection Diagram in the Configuration of HDI for Cloud (In the cluster configuration / BMC and Management SW connection configuration)

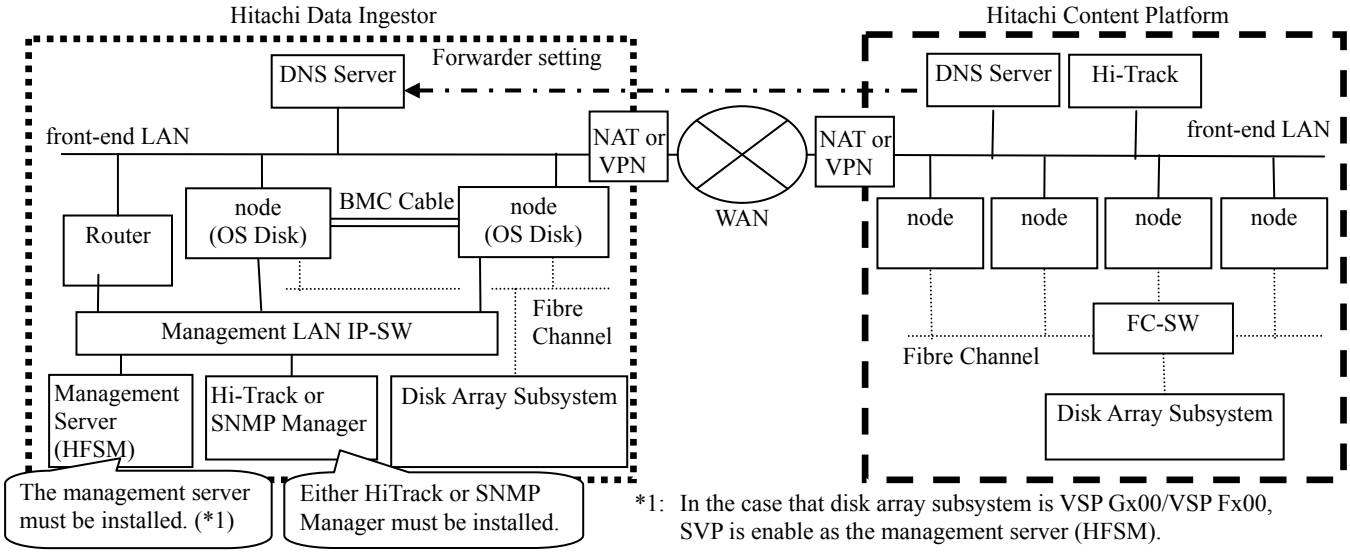


Figure 2.2-4 Overview of Connection Diagram in the Configuration of HDI for Cloud (In the cluster configuration / BMC direct connection configuration)

Copyright © 2010, 2016, Hitachi, Ltd.

(3-2) The configuration of HDI for cloud in the single node configuration

Figure 2.2-5 shows the overview of connection diagram of the configuration of HDI for Cloud in the single node configuration which is not connected to the disk array. In the case connected to the disk array, node and disk array are directly connected.

The functions are linked via WAN on the HDI side and the HCP side.

Note that the DNS server on the HDI side needs to set a forwarder for the DNS server on the HCP side. By setting the forwarder, even if the failover is done on the node of HCP due to a failure, the communication to HCP can be resumed as soon as the DNS server is updated.

The site on the HCP side must be the HCP-alone configuration, not the configuration of HDI for HCP.

Refer to "Installation '1.1.4 Overall configuration diagram (4) Overall system configuration diagram in the configuration of HDI for Cloud (single node)' (INST 01-0078)" for the entire system configuration figure, and refer to "A.2.3 LAN Cable" for the details of cable connection.

Note that, the dotted parts and the dashed parts in the figure show system ranges.

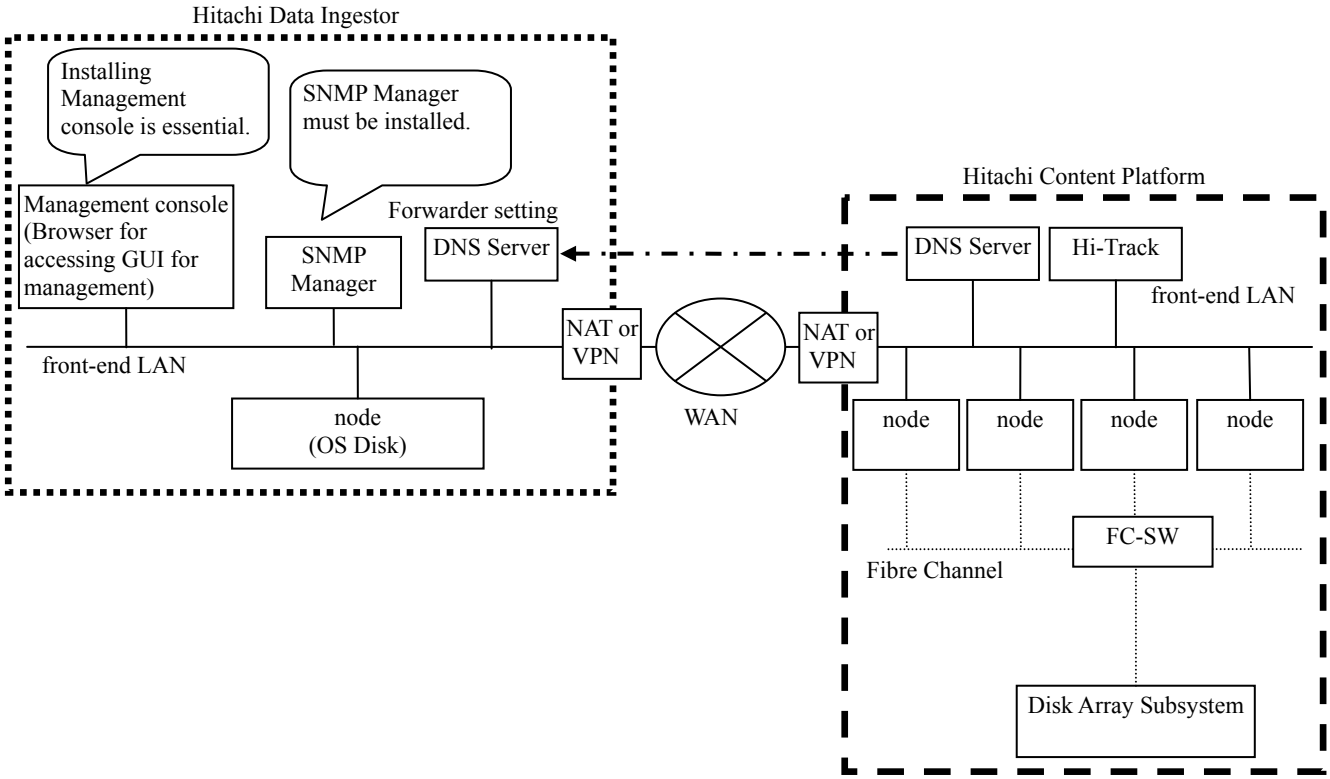


Figure 2.2-5 Overview of Connection Diagram in the Configuration of HDI for Cloud (In the single node configuration)

Copyright © 2010, 2012, Hitachi, Ltd.

(4) Configuration of the single node with spare for Cloud
It is the configuration to build the Active-Standby system using the multiple single nodes linked to HCP.
It only supports the single node configuration which not connecting to the disk array system.
Standby node is a backup node to switch the operation node in case of a failure occurred in the Active node.
When a failure occurred in the Active node, service is resumed by carrying over HCP data to the Standby node. In preparation for a failure, this stand-by single node configuration waits with the initial setups (including initial installation and management IP address setting) have been performed.
Note that the switch over between Active node and Standby node is performed manually.
Building, configuration and switchover of this configuration are performed by the system administrator.
The Active node and the Standby node of the Configuration of the single node with spare for Cloud need to be connected to the same network. Also, hardware configuration, software configuration and version need to be identical.
All single nodes included in this configuration completed the initial setup and also unique values have been set to IP address and host name of each single node.
Note that the DNS server on the HDI side needs to set a forwarder for the DNS server on the HCP side. By setting the forwarder, even if the failover is done on the node of HCP due to a failure, the communication to HCP can be resumed as soon as the DNS server is updated.
The site on the HCP side must be the HCP-alone configuration, not the configuration of HDI for HCP.
The dotted parts and the dashed parts in the figure show system ranges.

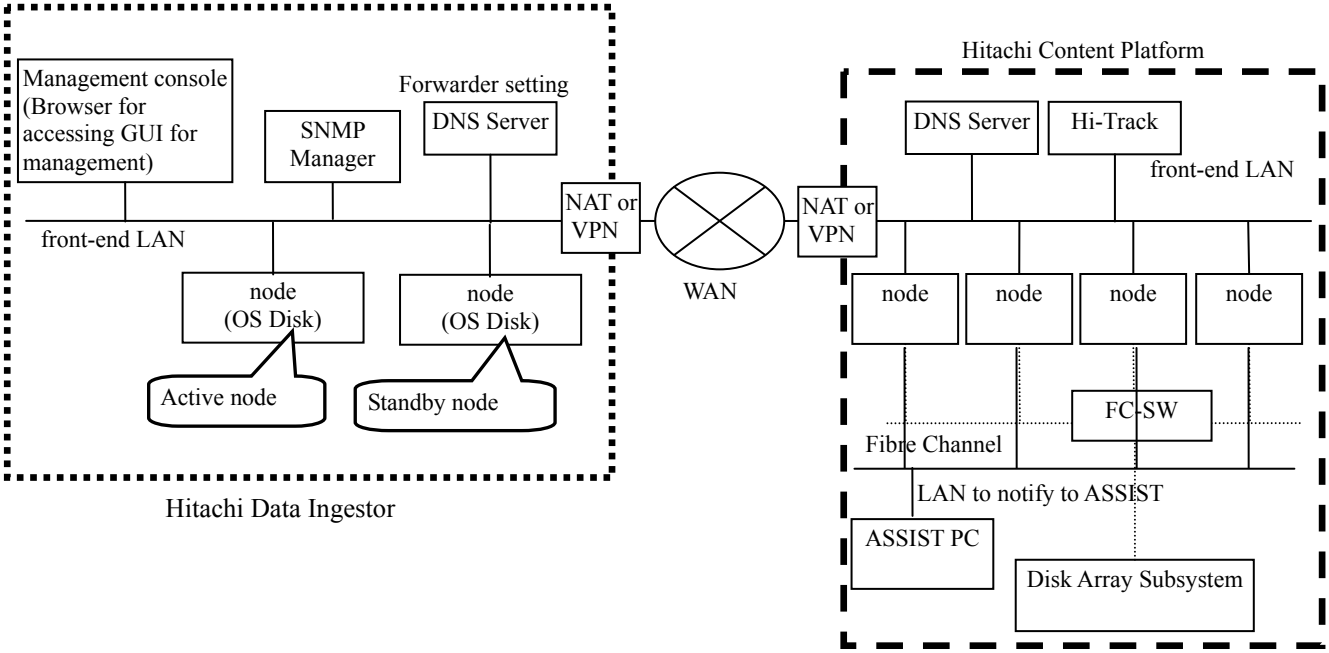


Figure 2.2-6 Overview of Connection Diagram in the Configuration of the single node with spare for Cloud

Copyright © 2010, 2016, Hitachi, Ltd.

2.3 Linking the HDI and the HCP

2.3.1 HCP functions: Namespaces and tenants

The Hitachi Content Platform (HCP) is a networking storage system which is suitable for the long storage of stored data without any modifications.

To ensure the integrity of stored data, the HCP uses Write Once Read Many (WORM) storage technology, protection policies, storage policies, and various metadata. In addition to easily accessing an archive when adding or retrieving data, the HCP can delete the saved data if permitted by the access right and policy.

The inside of HCP is divided into “tenant” and its lower place called “namespace”, which are logically partitioned and controlled.
Because objects stored in a namespace cannot be referenced from other namespaces, data saved for a different application, a business unit, or a customer can be separated.

Copyright © 2010, 2015, Hitachi, Ltd.

2.3.2 Linking the HDI and the HCP

When the HDI is linked with the HCP, files stored on an HDI file system using the NFS/CIFS protocol can be migrated automatically to the HCP according to a migration policy.
The migrated files are regularly stubbed by HDI, the clients can still read/write files while the HDI can reduce the capacity used in the file system.
When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default : 10%), HDI select WORM files and the files that update time is old, and stub them.

If HDI fails and the stub files are lost, the stub files can be restored from the data stored in the HCP. For the summary of the recovery procedure, refer to Theory "3.2.6 Restoration of Data in the File System in the cluster configuration" (THEO 03-0200) in the cluster configuration, and Theory "3.2.7 Restoration of Data in the node in the single node configuration" (THEO 03-0210) in the single node configuration.

Usually, one HCP tenant is allocated to one HDI for migration, but when the OS version is 4.0.0-XX or later, one HCP tenant can be allocated to two or more HDIs for migration. Migration can be done from one file system to only one namespace. When the OS version is 5.0.0-XX or later, one HCP namespace can be allocated to one directory immediately under the mount point of the file system. Multiple HDIs can access the namespace of HCP where data was migrated in the case of referring the migrated data.

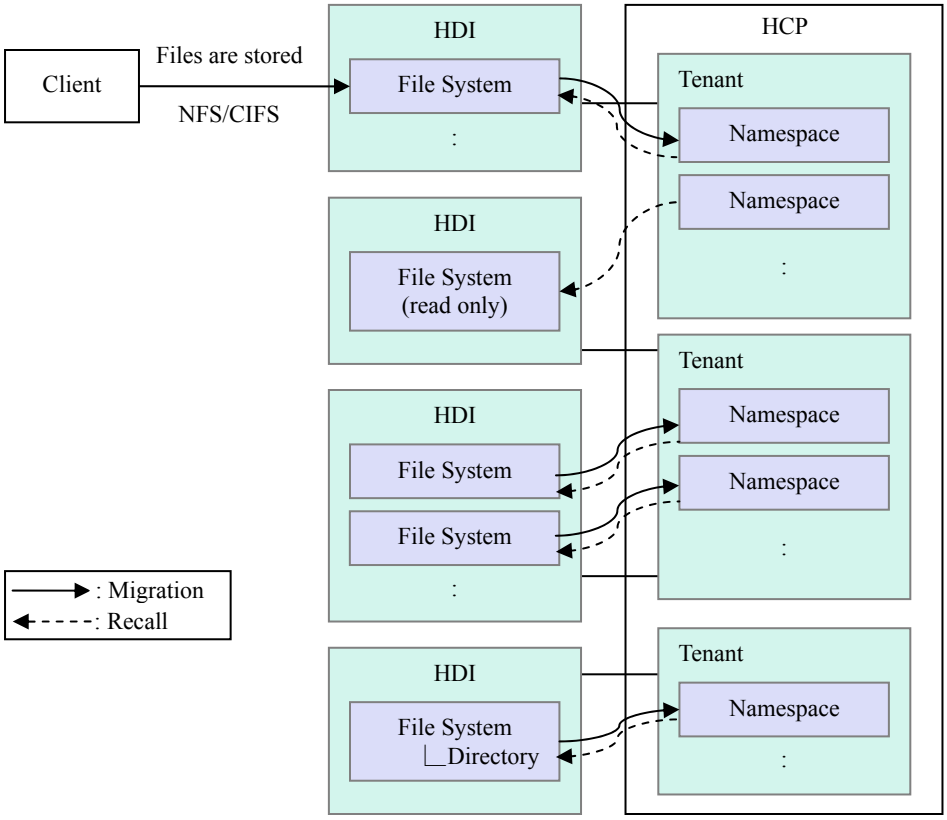


Figure 2.3.2-1 Relationship Between the HDI and the HCP1

Copyright © 2010, 2015, Hitachi, Ltd.

When the OS version 5.2.0-XX or later, data can be shared between multiple file systems on different HDI through one namespace. The end-user can read/write the same file from the other HDI (Read Write Content Sharing function. This function is abbreviated to RWCS.).

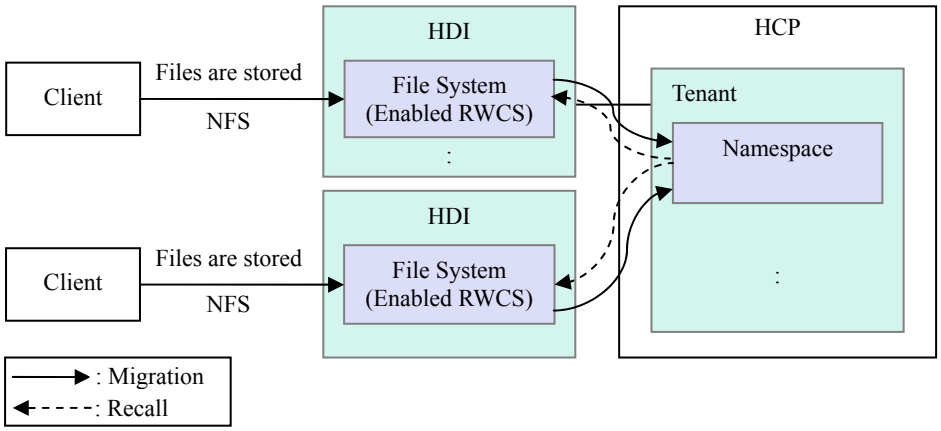


Figure 2.3.2-2 Relationship Between the HDI and the HCP2

Copyright © 2015, Hitachi, Ltd.

2.3.3 Failure notice method in the configuration of HDI for HCP

(1) The configuration of HDI for HCP (In the cluster configuration)
For the failure notice in the configuration of HDI for HCP in the cluster configuration, as shown in Figure 2.3.3-1, a failure is notified from each of the node of HDI and the node of HCP.
Note that if a failure occurred in the front-end LAN, a notice might be issued from both.
Figure 2.3.3-1 shows an example when a failure occurs in node 0 of HDI or node 0 of HCP.
In single node configuration, failures are normally notified to SNMP Manager which is for failure detection of single node. However, if there has been already Hi-Track for failure detection of HCP, failures can be notified to Hi-Track.

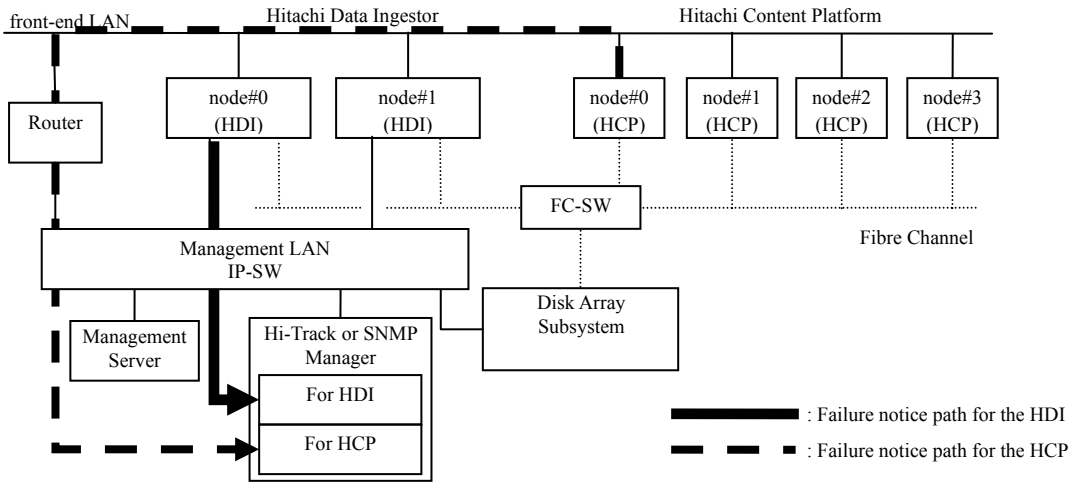


Figure 2.3.3-1 Failure Notice Path (in the configuration of HDI for HCP)

Copyright © 2010, 2012, Hitachi, Ltd.

(2) The configuration of HDI for Cloud (In the cluster configuration)
For a failure notice in the configuration of HDI for Cloud in the cluster configuration, as shown in Figure 2.3.3-2, failures occurred in respective sites are notified to Hi-Track installed in respective sites.
Figure 2.3.3-2 shows an example when failures occurred in node0 of HDI and node0 of HCP.
Since Hi-Track is not installed in single node configuration, failures occurred in HDI are notified to SNMP Manager.

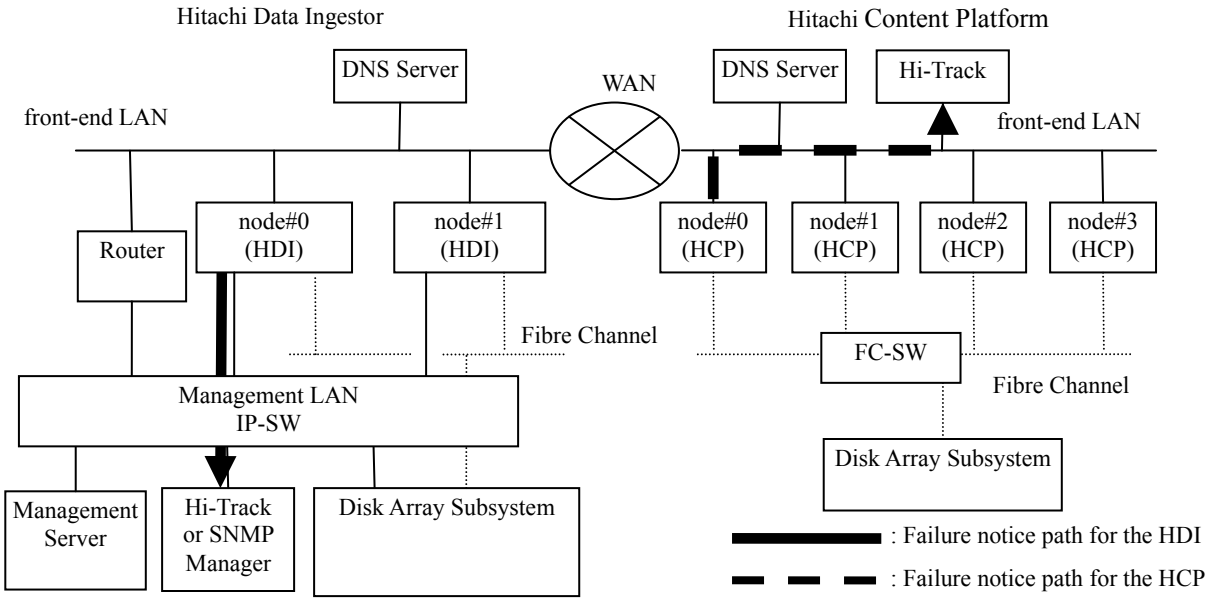


Figure 2.3.3-2 Failure Notice Path (in the configuration of HDI for Cloud)

Copyright © 2010, 2012, Hitachi, Ltd.

2.4 Software Specifications

2.4.1 Software and firmware lists

Table 2.4.1-1 shows the software installed in the HDI node. Table 2.4.1-2 shows the list of firmware.

Table 2.4.1-1 List of Software

No.	Name	Description
1	OS (File Operating System)	A program which receives Read/Write requests using NFS/CIFS protocol and provides file sharing for clients. Installed in an internal drive of node.
2	MIACAT	A program which notifies monitoring information of hardware collected by BMC to the OS.

Table 2.4.1-2 List of Firmware

No.	Name	Description
1	BIOS	A program which controls the hardware of node to provide basic input/output functions for the OS.
2	BMC firmware	This program controls the BMC settings.
3	HBA firmware (*1)	This program controls the HBA settings.
4	RAID controller firmware	This program controls the RAID controller.

*1: In the single node configuration not connected to the disk array, this component is not included.

Copyright © 2010, 2017, Hitachi, Ltd.

2.4.2 Data configuration

A RAID group is created in an internal drive in the node of HDI.

In the cluster configuration, the virtual disk is considered as the RAID1 configuration and has redundancy to a failure of one drive.

In the single node configuration, the virtual disk is considered as the RAID6 configuration and has redundancy to a failure of up to two drives.
However, in the single-node configuration connected to the disk array, it is configured as the RAID1.

In the cluster configuration, an OS disk is created in the internal drive and stores OS data.

In the single node configuration not connected to the disk array, an OS area and a user area are configured in the internal drive, and OS data and user data are stored respectively.

In the single node configuration connected to the disk array, an OS area is configured in the internal drive and OS data is stored there.

Figure 2.4.2-1 shows the schematic figure of an internal drive in the cluster configuration.

Figure 2.4.2-2 shows the schematic figure of an internal drive in the single node configuration (in the case of CR220SM and D51B-2U).

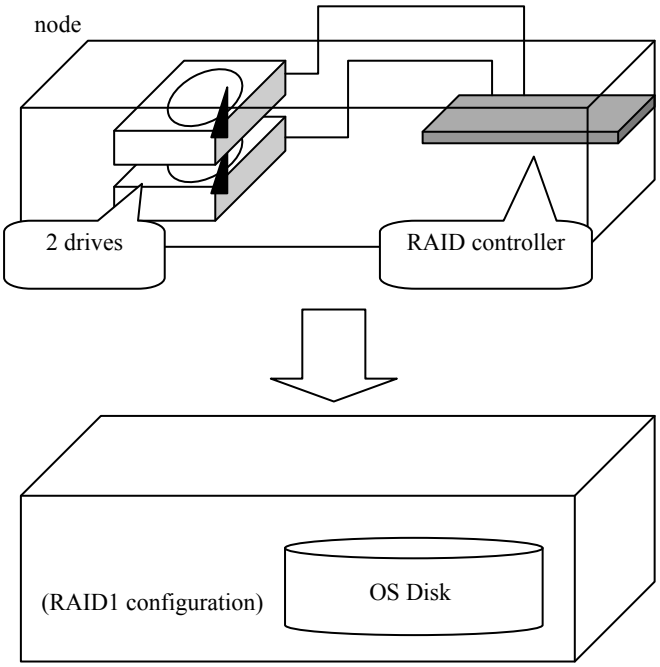


Figure 2.4.2-1 Schematic figure of an Internal drive (In the cluster configuration)

Copyright © 2011, 2016, Hitachi, Ltd.

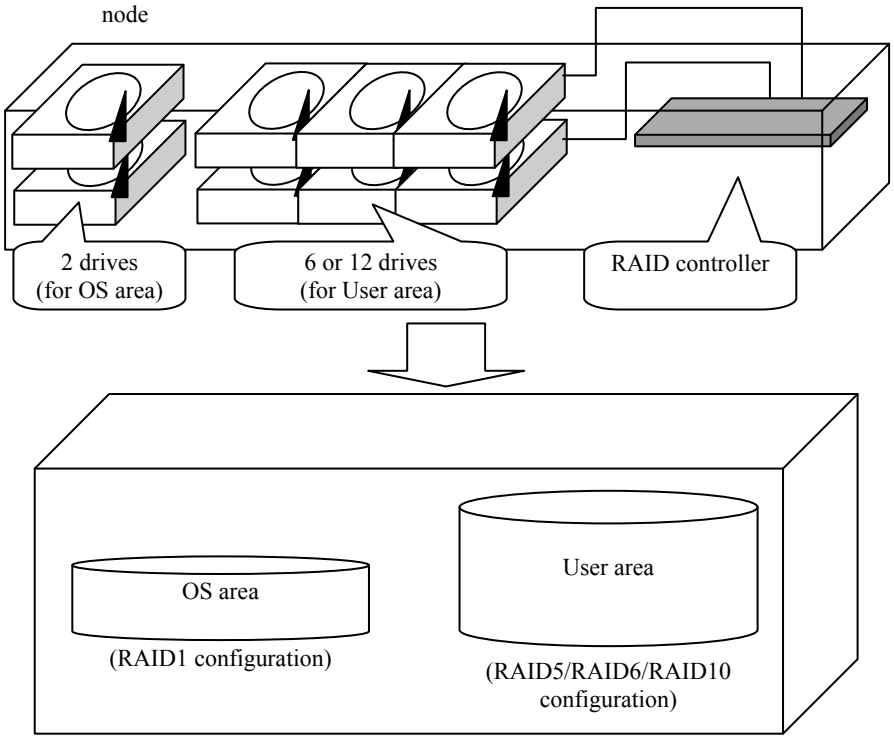


Figure 2.4.2-2 Schematic figure of an Internal drive in the single node configuration (in the case of CR220SM and D51B-2U)

Copyright © 2011, 2016, Hitachi, Ltd.

2.5 Disk Array Combination Function

2.5.1 List of disk array program products combination support that is supported by HDI

HDI can collaborate with the functions of the disk array (PP: Program Product).

Tables from 2.5.1-1 to 2.5.1-5 show the PPs of the disk array supported by HDI.

Confirm the currently used disk array subsystem and refer to the corresponding table.

Table 2.5.1-1 Program Products of AMS2000/MSS series that are supported by HDI

No.	Program product name	Collaboration with HDI
1	Cache Residency Manager	Not supported
2	Performance Monitor	Supported
3	Cache Partition Manager	Supported
4	LUN Manager	Supported
5	Dynamic Provisioning	Supported
6	Data Retention Utility	Not supported
7	Copy-on-Write Snapshot	Not supported
8	ShadowImage in-system Replication	Supported
9	TrueCopy remote replication	Supported
10	TrueCopy Extended Distance	Supported
11	True Copy Modular Distributed	Not supported
12	Modular Volume Migration	Not supported
13	Account Authentication	Supported
14	Audit Logging	Not supported
15	Power Saving	Not supported
16	Tray Power Saving	Not supported
17	Command Control Interface	Supported
18	SNMP Agent Support Function	Not supported
19	Password Protection	Not supported
20	Long Life Support Indicator	Not supported
21	Hitachi Storage Navigator Modular 2	Supported
22	LUN Expansion	Supported
23	Dynamic Tiering	Not supported
24	Fibre Channel Option	Not supported

Copyright © 2010, 2013, Hitachi, Ltd.

Table 2.5.1-1-2 Program Products of HUS100 Series that are supported by HDI

No.	Program product name	Collaboration with HDI
1	Cache Residency Manager	Not supported
2	Performance Monitor	Supported
3	Cache Partition Manager	Supported
4	LUN Manager	Supported
5	Dynamic Provisioning	Supported
6	Data Retention Utility	Not supported
7	Copy-on-Write Snapshot	Not supported
8	ShadowImage in-system Replication	Supported
9	TrueCopy remote replication	Supported
10	TrueCopy Extended Distance	Supported
11	True Copy Modular Distributed	Not supported
12	Modular Volume Migration	Not supported
13	Account Authentication	Supported
14	Audit Logging	Not supported
15	Power Saving	Not supported
16	Tray Power Saving	Not supported
17	Command Control Interface	Supported
18	SNMP Agent Support Function	Not supported
19	Password Protection	Not supported
20	Long Life Support Indicator	Not supported
21	Hitachi Storage Navigator Modular 2	Supported
22	LUN Expansion	Supported
23	Dynamic Tiering	Supported
24	Fibre Channel Option	Supported

Copyright © 2011, 2013, Hitachi, Ltd.

Table 2.5.1-3 Program Products of USP V/USP VM that are supported by HDI

No.	Program product name	Collaboration with HDI
1	Cache Residency Manager	Not supported
2	Command Control Interface	Supported
3	Copy-on-Write Snapshot	Not supported
4	DB Validator	Not supported
5	Dynamic Provisioning	Supported
6	LUN Manager	Supported
7	Data Retention Utility	Not supported
8	Performance Monitor	Supported
9	ShadowImage	Supported
10	SNMP Agent	Not supported
11	Storage Navigator	Supported
12	TrueCopy asynchronous extension	Supported
13	TrueCopy	Supported
14	Universal Replicator	Supported
15	Universal Volume Manager	Supported
16	Virtual LVI	Supported
17	Virtual Partition Manager	Supported
18	Volume Migration	Supported
19	Volume Shredder	Supported
20	Compatible PAV	Not supported
21	Volume Retention Manager	Not supported
22	Open Volume Management	Not supported (*1)
23	Compatible Mirroring for IBM FlashCopy	Not supported
24	Volume Security	Not supported
25	Volume Security Port Option	Not supported
26	Compatible Replication for IBM XRC	Not supported
27	TrueCopy Sync and full function HUR with 3DC and 4x4	Not supported
28	Compatible Hyper PAV	Not supported
29	FICON Data Migration	Not supported
30	Encrypt License Key	Not supported
31	High Availability Manager	Not supported
32	Compatible High Performance Connectivity for IBM FICON Software	Not supported
33	Configuration File Loader	Supported

*1: Although the combination function with the OS is not supported, maintenance personnel can use it because it is required for LDEV creation.

Copyright © 2010, 2013, Hitachi, Ltd.

Table 2.5.1-4 PPs for VSP/VSP G1000 supported by HDI

No.	Program product name	Collaboration with HDI and VSP	Collaboration with HDI and VSP G1000
1	Cache Residency Manager	Not supported	Not supported
2	Command Control Interface	Supported	Supported
3	Copy-on-Write Snapshot	Not supported	
4	Dynamic Provisioning	Supported	Supported
5	LUN Manager	Supported	Supported
6	Data Retention Utility	Not supported	Not supported
7	Performance Monitor	Supported	Supported
8	Server Priority Manager	Not supported	Not supported
9	ShadowImage	Supported	Supported
10	Storage Navigator	Supported	Supported
11	TrueCopy	Supported	Supported
12	Universal Replicator	Supported	Supported
13	Universal Volume Manager	Supported	Supported
14	Virtual LVI	Supported	Supported
15	Virtual Partition Manager	Supported	Supported
16	Volume Migration	Supported	Supported
17	Volume Shredder	Supported	Supported
18	Compatible PAV	Not supported	Not supported
19	Volume Retention Manager	Not supported	Not supported
20	Open Volume Management	Not supported (*1)	Not supported (*1)
21	Compatible Mirroring for IBM FlashCopy	Not supported	Not supported
22	Volume Security	Not supported	Not supported
23	Volume Security Port Option	Not supported	Not supported
24	Compatible Replication for IBM XRC	Not supported	Not supported
25	Disaster Recovery Extended	Not supported	Not supported
26	Compatible Hyper PAV	Not supported	Not supported
27	FICON Data Migration	Not supported	Not supported
28	Encryption License Key	Supported	Supported
29	High Availability Manager	Not supported	
30	Compatible High Performance Connectivity	Not supported	Not supported
31	Dynamic Tiering	Supported	Supported
32	Configuration File Loader	Supported	Supported
33	H-UVM		Not Supported
34	Thin Image		Not Supported
35	global-active device (*2)		Not Supported
36	nondisruptive migration Software		Not Supported

*1: Although the combination function with the OS is not supported, maintenance personnel can use it because it is required for LDEV creation.

*2: P.P that uses the global storage virtualization function.

Copyright © 2010, 2016, Hitachi, Ltd.

Table 2.5.1-5 PPs for HUS VM supported by HDI

No.	Program product name	Collaboration with HDI
1	Cache Residency Manager	Not supported
2	Dynamic Provisioning	Supported
3	LUN Manager	Supported
4	Data Retention Utility	Not supported
5	Performance Monitor	Supported
6	ShadowImage	Supported
7	SNMP Agent	Not supported
8	Storage Navigator	Supported
9	TrueCopy	Supported
10	Universal Replicator	Supported
11	Universal Volume Manager	Supported
12	Virtual Partition Manager	Supported
13	Volume Migration	Supported
14	Volume Shredder	Supported
15	Dynamic Tiering	Supported
16	Audit Log	Not supported
17	LUN Expansion	Supported
18	Virtual LUN	Supported

Copyright © 2010, 2013, Hitachi, Ltd.

Table 2.5.1-6 PPs for VSP Gx00/VSP Fx00 supported by HDI

No.	Program product name	Collaboration with HDI and VSP Gx00	Collaboration with HDI and VSP Fx00
1	Dynamic Provisioning	Supported	Supported
2	LUN Manager	Supported	Supported
3	Data Retention Utility	Not supported	Not supported
4	Performance Monitor	Supported	Supported
5	Server Priority Manager	Not supported	Not supported
6	ShadowImage	Not supported	Not supported
7	Storage Navigator	Supported	Supported
8	TrueCopy	Not supported	Not supported
9	Universal Replicator	Not supported	Not supported
10	Universal Volume Manager	Supported	Not supported
11	Virtual Partition Manager	Supported	Not supported
12	Volume Shredder	Supported	Not supported
13	Open Volume Management	Not supported (*1)	Not supported (*1)
14	Encryption License Key	Supported	Supported
15	Dynamic Tiering	Supported	Not supported
16	Thin Image	Not supported	Not supported
17	Volume Migration V2	Supported	Not supported
18	SNMP Agent	Not supported	Not supported
19	Resource Partition Manager	Not supported	Not supported
20	global-active device(*2)	Not Supported	Not supported
21	Active Flash	Supported	Not supported
22	nondiscruptive migration	Not supported	Not supported

*1: Although the combination function with the OS is not supported, maintenance personnel can use it because it is required for LDEV creation.

*2: P.P that uses the global storage virtualization function.

NOTE: For details, refer “Function Release Schedule” of HDI.

Copyright © 2015, 2018, Hitachi, Ltd.

2.6 Network Specifications

For details about the network specifications for the Private Maintenance port, Heartbeat port, Management port, Data port, and BMC port used for the HDI nodes, refer to Theory "Chapter 5 LAN Configuration Settings" (THEO 05-0000).

2.6.1 Cluster configuration

In the cluster configuration, each node has the LAN interfaces shown in Table 2.6.1-1, and these LAN interfaces are connected as shown in Figure 2.6.1-1. In addition, each port supports different protocols (IPv4/IPv6). For the BMC direct connection configuration, refer to Figure 2.6.1-2.

The IP addresses shown in Table 2.6.1-2 must be set for each node, and the LAN interface must be segmented as shown in the "Network" column of the table.

In the BMC and Management SW connection configuration, the PC shown in Table 2.6.1-3 must also be connected to the management LAN IP-SW.

Table 2.6.1-1 LAN Interfaces of a node

Port name (Interface name)	Usage	IP Address	
		IPv4	IPv6
Private Maintenance port (pm0)	Port used by maintenance personnel	Yes (essential)	Yes
Heartbeat port (hb0)	Port for heartbeat between nodes	Yes (essential)	No
Management port (mng0)	Port for communication with the HFSM and for heartbeat between nodes	Yes (essential)	Yes
Data port (ethX) (*2)	Port used by a customer	Yes	Yes
BMC port (bmc0) (*1)	Port for controlling the cluster	Yes (essential)	No
Reset port (pm1) (*1)	Port for reset (in the BMC direct connection configuration)	Yes (essential)	No

*1: In the BMC direct connection configuration, the same IP address will be set automatically to BMC port and Reset port.

*2: When using a 10GbE card, the interface name will be "xgben" ("n" is an integer greater than or equal to 0.)

Copyright © 2010, 2012, Hitachi, Ltd.

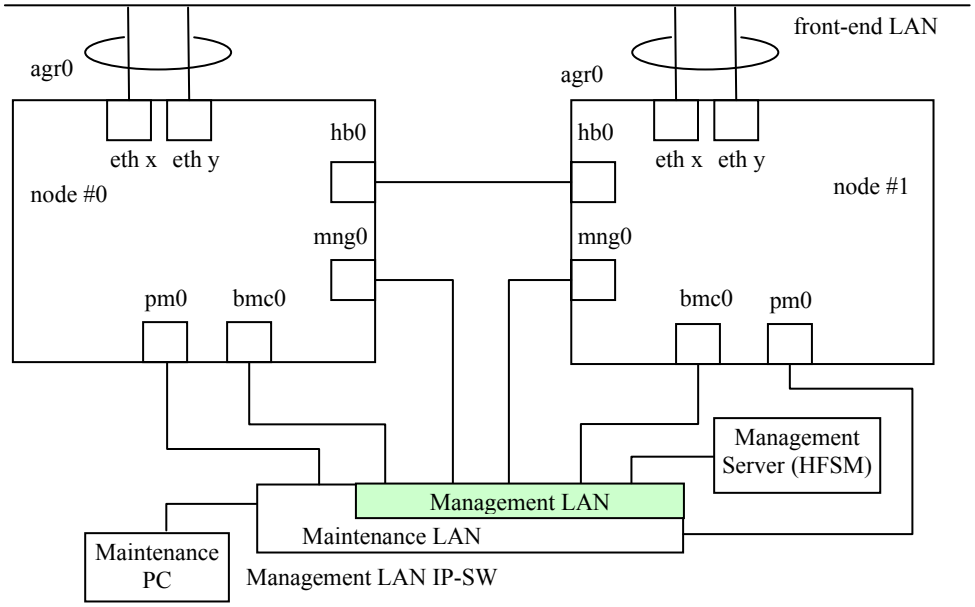


Figure 2.6.1-1 Network Connection Diagram (BMC and Management SW connection configuration)

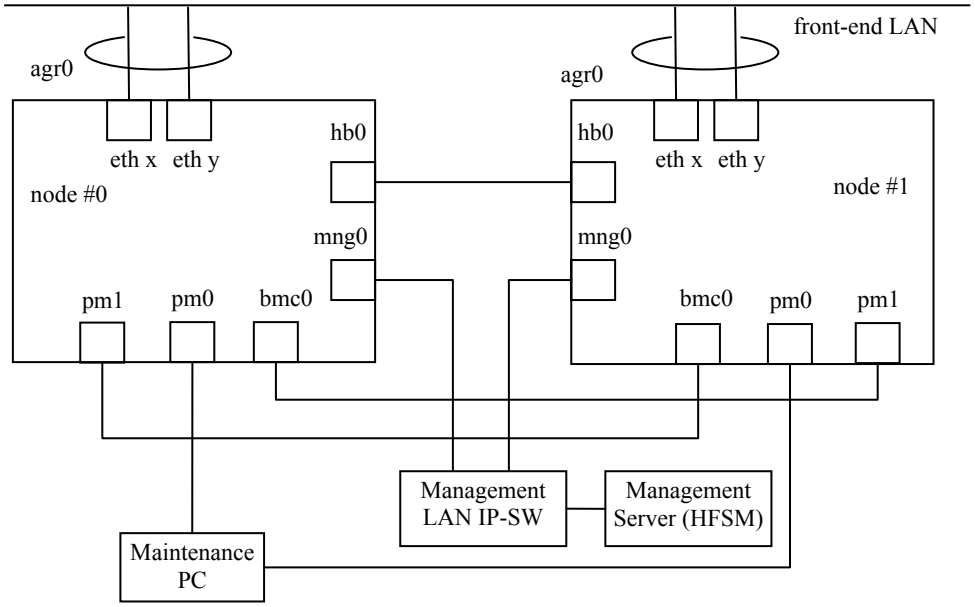


Figure 2.6.1-2 Network Connection Diagram (BMC direct connection configuration)

Copyright © 2011, 2012, Hitachi, Ltd.

Table 2.6.1-2 LAN Interface Networks

#	Port name	Interface name	Network
1	Private Maintenance port	pm0	1.Maintenance LAN
2	Heartbeat port	hb0	2.Heartbeat LAN
3	Management port	mng0	3.Management LAN
4	BMC port	bmc0	3.Management LAN
	(in the BMC direct connection configuration)		Direct connection for reset
5	Data port	eth n (*1) (“n” is an integer of 0 and above.)	4.front-end LAN
6			4.front-end LAN
7	Reset port (*2)	pm1	Direct connection for reset

*1: The name of interface becomes agr0 by performing link aggregation.
*2: Reset port is required only when the BMC direct connection configuration. In the BMC direct connection configuration, the number of IP segments that can be used in user LAN will be reduced by 1.

Table 2.6.1-3 PC Connected to the Management LAN IP-SW

#	Computer type	Network
1	Management server	3.Management LAN
2	Maintenance PC	1.Maintenance LAN

Copyright © 2012, Hitachi, Ltd.

2.6.2 Single node configuration

In the single node configuration, a node has the LAN interfaces shown in Table 2.6.2-1, and these LAN interfaces are connected as shown in Figure 2.6.2-1 or Figure 2.6.2-2. In addition, each port supports different protocols (IPv4/IPv6).

The IP addresses shown in Table 2.6.2-2 and Table 2.6.2-3 must be set.

Table 2.6.2-1 LAN Interfaces of a node

Port name (Interface name)	Usage	IP Address	
		IPv4	IPv6
Private Maintenance port (pm0)	Port used by maintenance personnel	Yes (essential)	Yes
Management port (mng0)	Port for initial setup/ Port used by a customer (*1)	Yes (essential)	Yes
Data port (ethX) (*2)	Port used by a customer (*1)	Yes	Yes

*1: In the configuration of using the management port, the Data port does not use. In the Configuration using trunk 2 Data ports, the management port is used only at the time of initial setup but the Data port is used in the operation.

*2: When using a 10GbE card, the interface name will be “xgben” (“n” is an integer greater than or equal to 0.)

Copyright © 2011, 2012, Hitachi, Ltd.

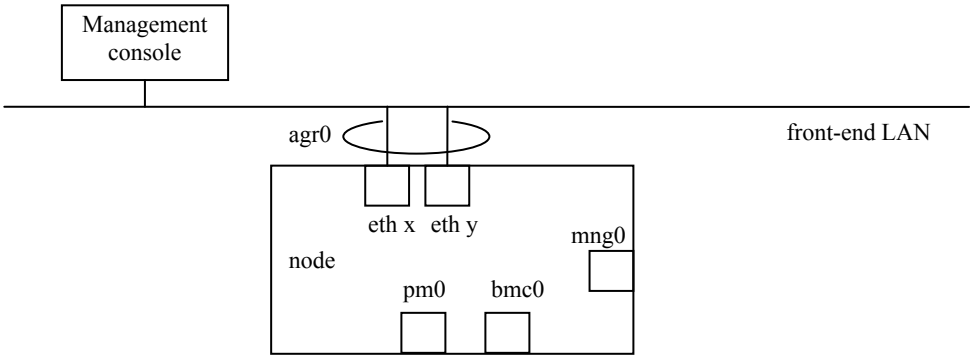


Figure 2.6.2-1 Network Connection Diagram (Configuration using trunk 2 Data ports)

Table 2.6.2-2 LAN Interface Networks

# (*1)	Port name	Interface name	Network
1	Private Maintenance port	pm0	1.Maintenance LAN
2	Management port (*2)	mng0	2.Management LAN
3	BMC port	bmc0	1.Maintenance LAN
4	Data port (*4)	eth x, eth y (*3) (“x”, “y” is an integer of 0 and above.)	3.front-end LAN

*1: Private Maintenance port and Management port should be different network segment.
*2: Connected from PC that has management GUI directly during initial setup wizard (for setting the Data port).
Connected to front-end LAN temporarily during system LU recovery (not used in user daily operation).
*3: The name of interface becomes agr0 by performing link aggregation.
*4: When using a 10GbE card, the interface name will be “xgben” (“n” is an integer greater than or equal to 0.)

Copyright © 2011, 2013, Hitachi, Ltd.

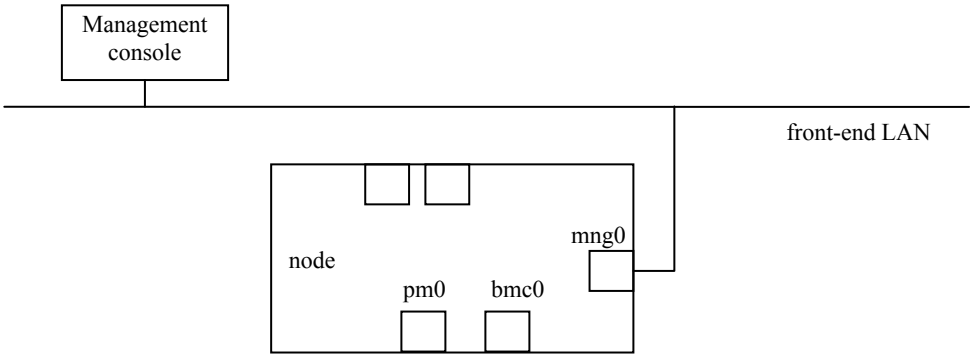


Figure 2.6.2-2 Network Connection diagram (Configuration using Management port)

Table 2.6.2-3 LAN Interface Networks

# (*1)	Port name	Interface name	Network
1	Private Maintenance port	pm0	1.Maintenance LAN
2	Management port	mng0	2.Management LAN
3	BMC port	bmc0	1.Maintenance LAN
4	Data port	Unused.	

*1: Each port should be different network segment.

Copyright © 2011, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, Hitachi, Ltd.

Chapter 3 Description of Operations

3.1 Specifications for Operations

3.1.1 Read/write processing from client

In the read/write processing in the configuration which is not connected to the disk array subsystem, file read/write is performed for the internal drive by the read/write requests from the client to the node.
The flow of the write processing in the configuration which is not connected to the disk array subsystem is shown in Figure 3.1.1-1 and the flow of the read processing in the configuration which is not connected to the disk array subsystem is shown in Figure 3.1.1-2.

In the read/write processing in the configuration which is connected to the disk array subsystem, file read/write is performed for the disk array subsystem by the read/write requests from the client to the node.
The flow of the write processing in the configuration which is connected to the disk array subsystem is shown in Figure 3.1.1-3 and the flow of the read processing in the configuration which is connected to the disk array subsystem is shown in Figure 3.1.1-4.

Figure 3.1.1-5 shows the write processing flow of the configuration of HDI for HCP, Figure 3.1.1-6 shows the read processing flow of the configuration of HDI for HCP.

Cluster configuration and single node configuration have a same flow of Read/Write.

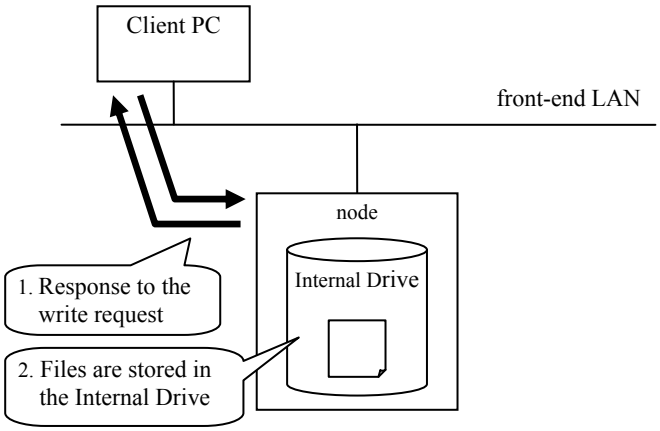


Figure 3.1.1-1 Flow of the write processing in the configuration (which is not connected to the disk array subsystem)

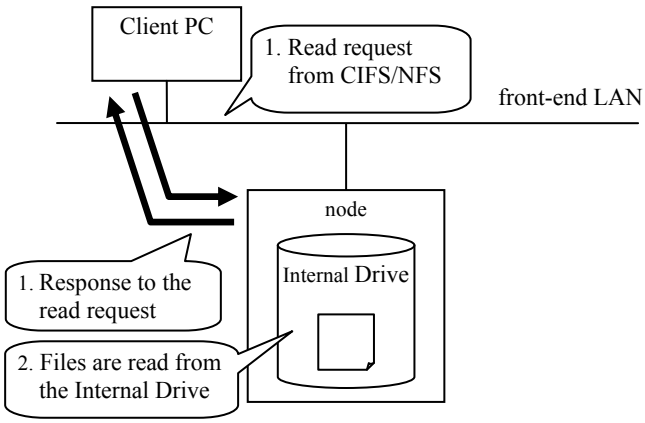


Figure 3.1.1-2 Flow of the read processing in the configuration (which is not connected to the disk array subsystem)

Copyright © 2010, 2016, Hitachi, Ltd.

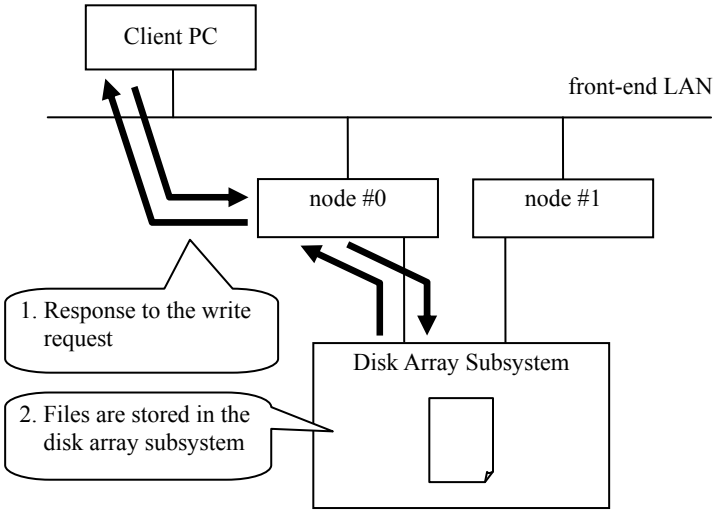


Figure 3.1.1-3 Flow of the write processing in the configuration (which is connected to the disk array subsystem)

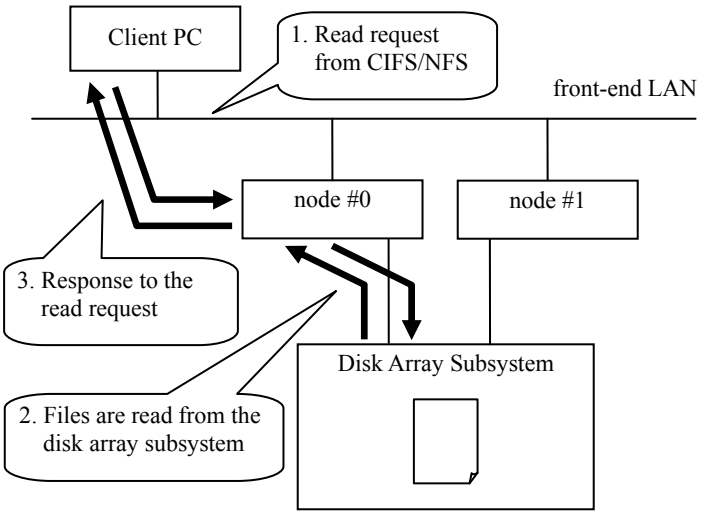


Figure 3.1.1-4 Flow of the read processing in the configuration (which is connected to the disk array subsystem)

Copyright © 2012, Hitachi, Ltd.

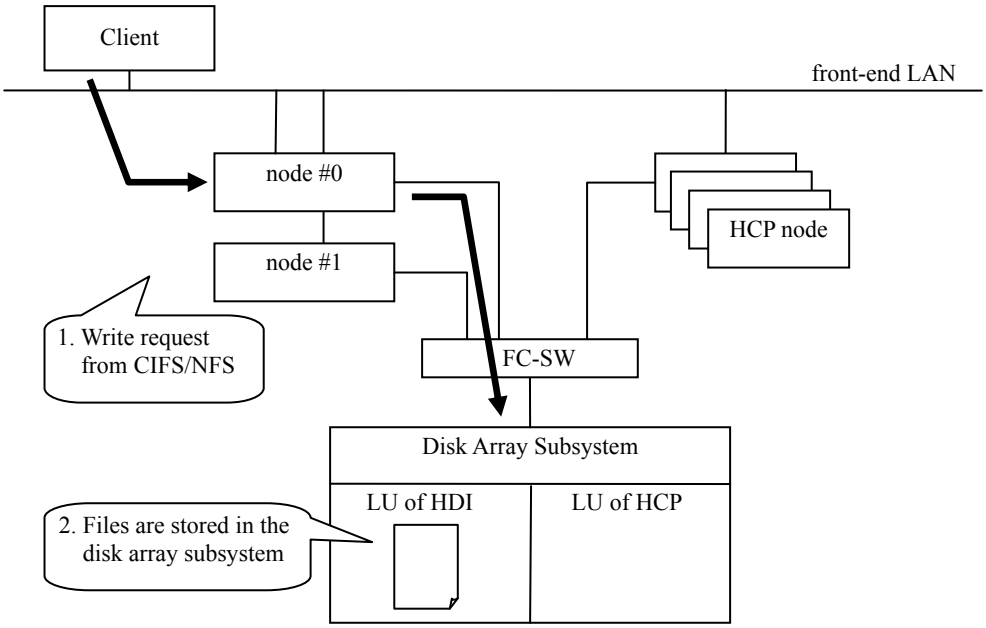


Figure 3.1.1-5 Flow of the write processing in the configuration of HDI for HCP

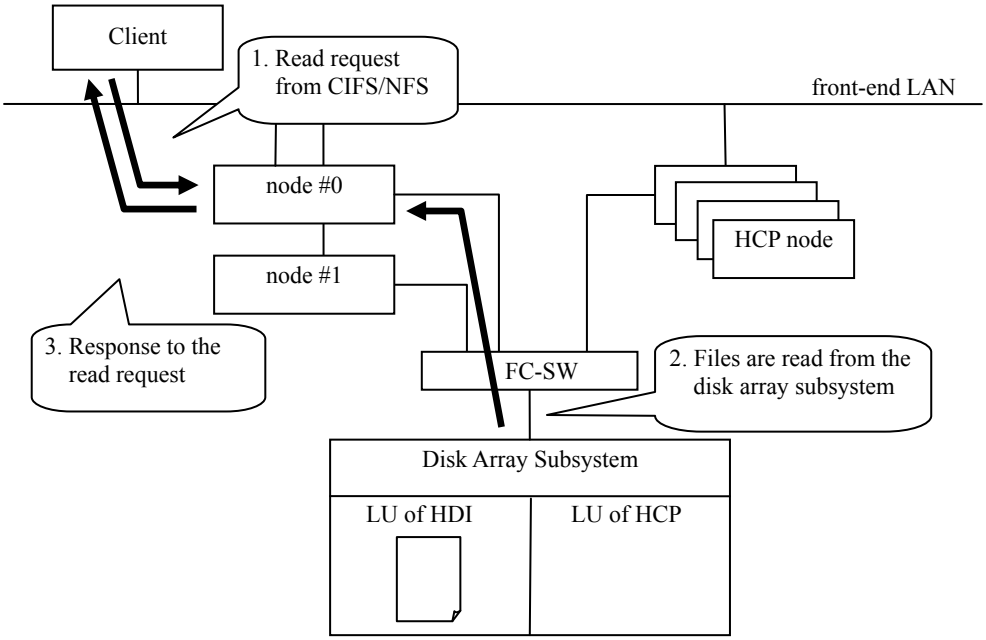


Figure 3.1.1-6 Flow of the read processing in the configuration of HDI for HCP

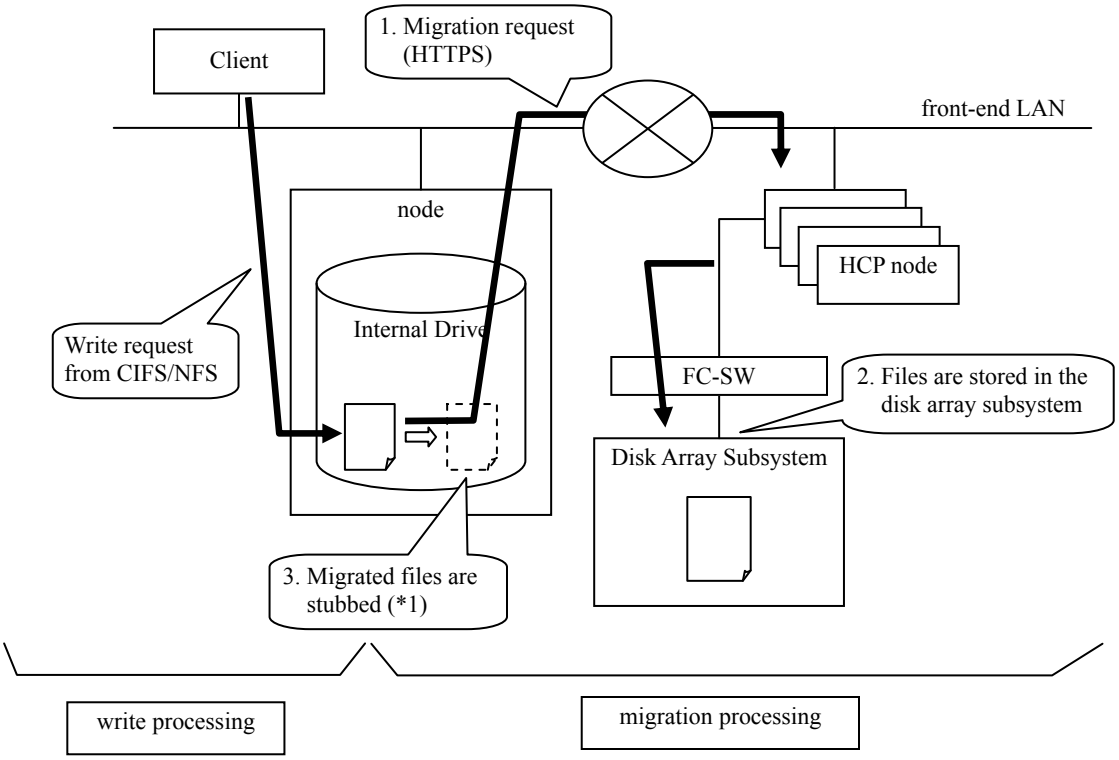
Copyright © 2010, 2012, Hitachi, Ltd.

3.1.2 Migration processing

The read/write processing in the single node configuration and in the configuration of HDI for HCP / HDI for Cloud in the cluster configuration includes migration and recall processing between HDI and HCP in addition of read/write from a client to HDI.
In the single node configuration, the migration processing is performed according to the migration policy specified in the GUI for management.
Figure 3.1.2-1 shows the migration processing flow in the configuration of HDI for Cloud, and the configuration of HDI for HCP has the same processing flow.

In the cluster configuration, the migration processing is performed according to the migration policy specified in HFSM.
Figure 3.1.2-2 shows the migration processing flow in the configuration of HDI for HCP, and the configuration of HDI for Cloud has the same processing flow.

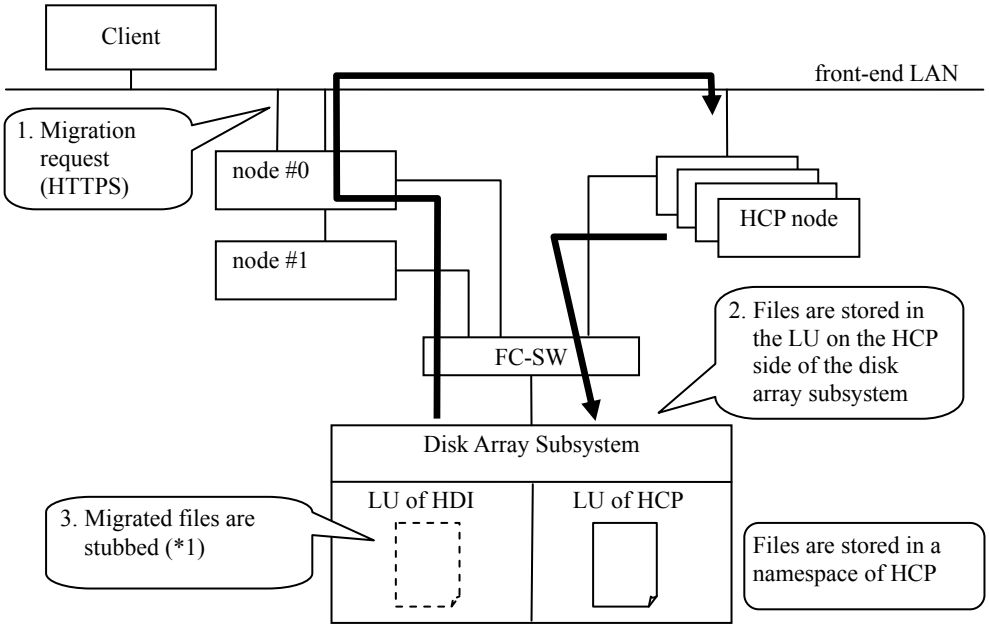
The migration processing flow in the single node configuration which is connected to the disk array is the same as in the case of the cluster configuration.



*1: When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default : 10%), the files are stubbed in chronological order of the last update dates and time.

Figure 3.1.2-1 Migration processing in the single node configuration when not connected to the disk array subsystem

Copyright © 2010, 2016, Hitachi, Ltd.



*1: When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default : 10%), the files are stubbed in chronological order of the last update dates and time.

Figure 3.1.2-2 Migration Processing When the Configuration of HDI for HCP

Copyright © 2011, Hitachi, Ltd.

3.1.3 Recall processing

Recall processing is executed when a migrated stub file is accessed by a client.

Figure 3.1.3-1 shows the recall processing flow to be executed when reading the stub file in the single node configuration which is not connected to the disk array subsystem.

The recall processing flow of reading a stub file in HDI in the cluster configuration is shown in Figure 3.1.3-2 and the flow of writing to a stub file is shown in Figure 3.1.3-3.

Note that Figure 3.1.3-2 and Figure 3.1.3-3 show the processing flow in the cluster configuration, but the single node configuration which is connected to the disk array subsystem has the same processing flow.

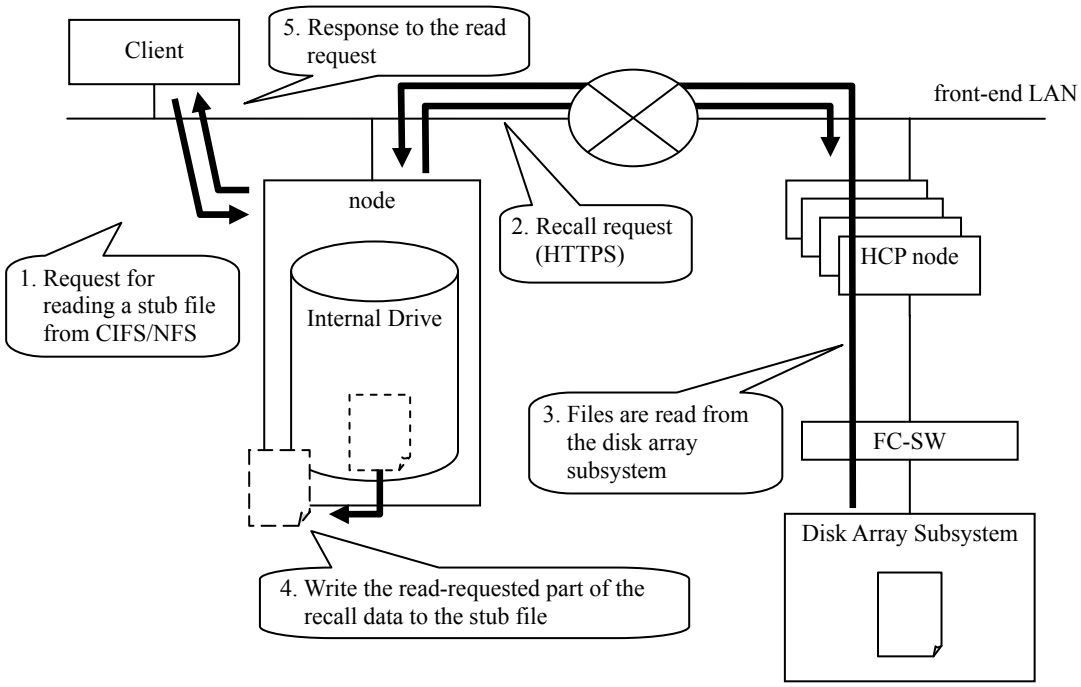


Figure 3.1.3-1 Recall processing in the single node configuration when not connected to the disk array subsystem

Copyright © 2010, 2016, Hitachi, Ltd.

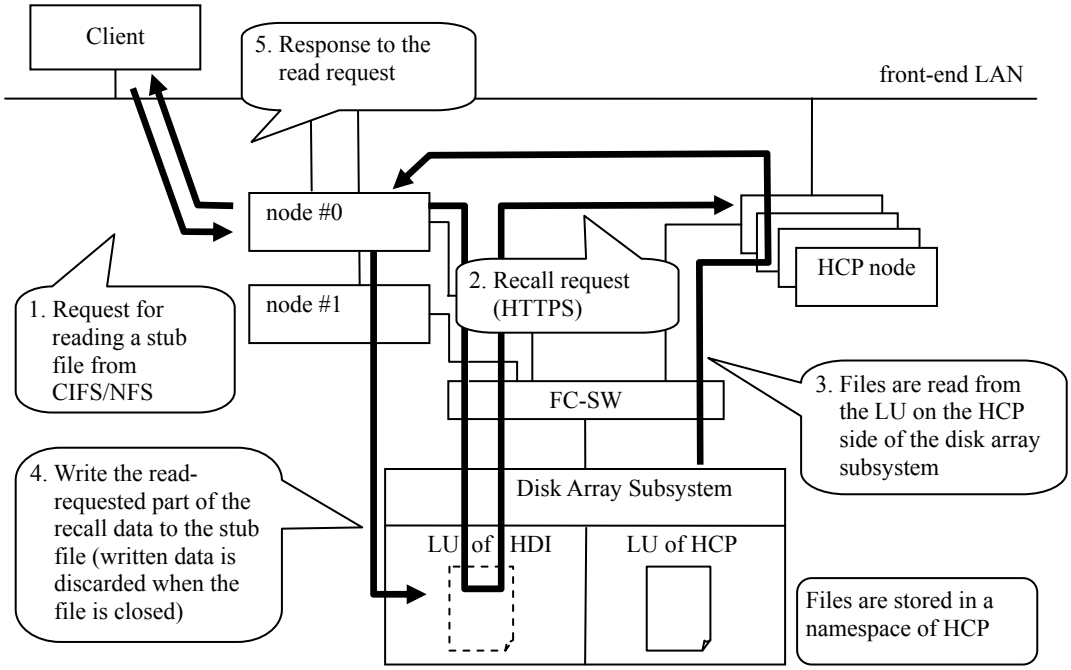


Figure 3.1.3-2 Recall Processing When the Configuration of HDI for HCP

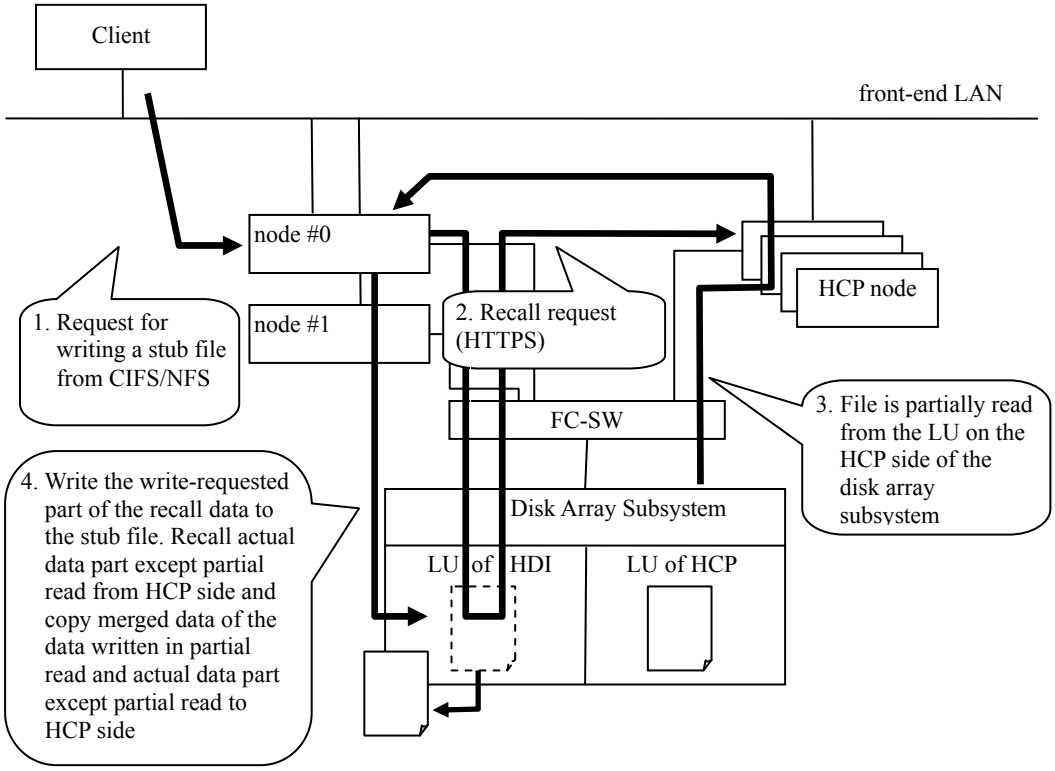


Figure 3.1.3-3 Flow of Entire Recall Processing on a write request

Copyright © 2010, 2011, Hitachi, Ltd.

3.1.4 Concept of HDI single node configuration

In the single node configuration, the resource group starts when OS starts, and the resource group terminates when OS terminates. If a failure occurs on the OS, the service is stopped until the failure recovery is completed unlike the cluster configuration.

NOTE: Because mounting of “data of the past version directory” is not synchronized with start-up of the resource groups for the OS version 5.1.0-XX and later, the mounting of “data of the past version directory” might not be complete although the start-up of the resource groups has been complete. In this case, the read/write operation for “data of the past version directory”, mounting of which has not been complete, fails for a moment.

3.1.5 Concept of HDI cluster and resource groups

(1) Configuration of cluster systems

In the cluster system configuration, when either node fails, the service can be continued by performing failover the service of HDI operated in the node to the paired node.
Furthermore, the node pairs monitor mutually, and when there is no response from either node, the function to stop the OS of the node forcibly by sending the Reset signal from the paired node and to failover exists.
Note that starting the recovery work early is recommended when a failure is detected. When the service of HDI is executed in either node by failover, the load is concentrated to the node and the performance may be deteriorated.
Figure 3.1.5-1 shows the concept of the cluster system configuration.

NOTE: Because mounting of “data of the past version directory” is not synchronized with start-up of the resource groups for the OS version 5.1.0-XX and later, the mounting of “data of the past version directory” on the migration target node to which a failover or failback has been performed might not be complete. In this case, the read/write operation for “data of the past version directory”, mounting of which has not been complete, fails for a moment.

(2) Characteristics of cluster systems

(a) A cluster is consisted of a node pair. Mutually monitoring the nodes in a cluster provides reliability. In a disk array subsystem, an alternate FC path and an alternate disk path are set considering failover in a cluster. By doing so, reliability of the entire system can be improved.

(b) Although there are access paths from both of two nodes to the User LU in the disk array subsystem, for preventing the access from both nodes at the same time, the exclusive access control is performed. If one node cannot continue services and the failover occurs, in-process data before writing to the User LU is discarded, and the services (Virtual IP, Data in the User LU in the disk array subsystem and others) are taken over to the paired node. Figure 3.1.5-2 shows the image figure of the resource group failover.
The client can resume the operation processing suspended after failover. Note that, for the CIFS connection, reconnection from the client side is mandatory, but for the NFS connection, read/write can be performed without reconnection depending on the option use.

Copyright © 2010, 2014, Hitachi, Ltd.

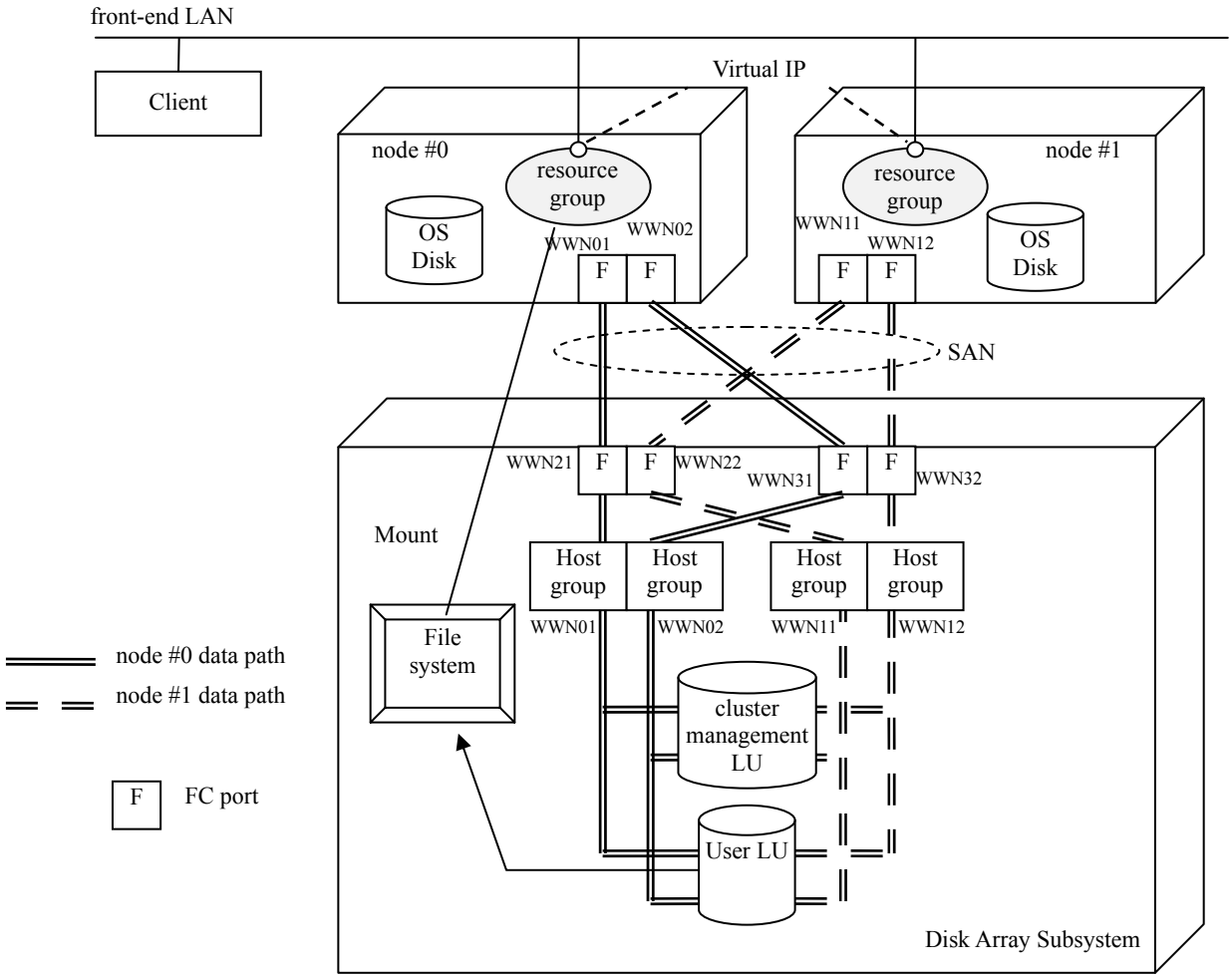


Figure 3.1.5-1 Concept of the Cluster System for HDI

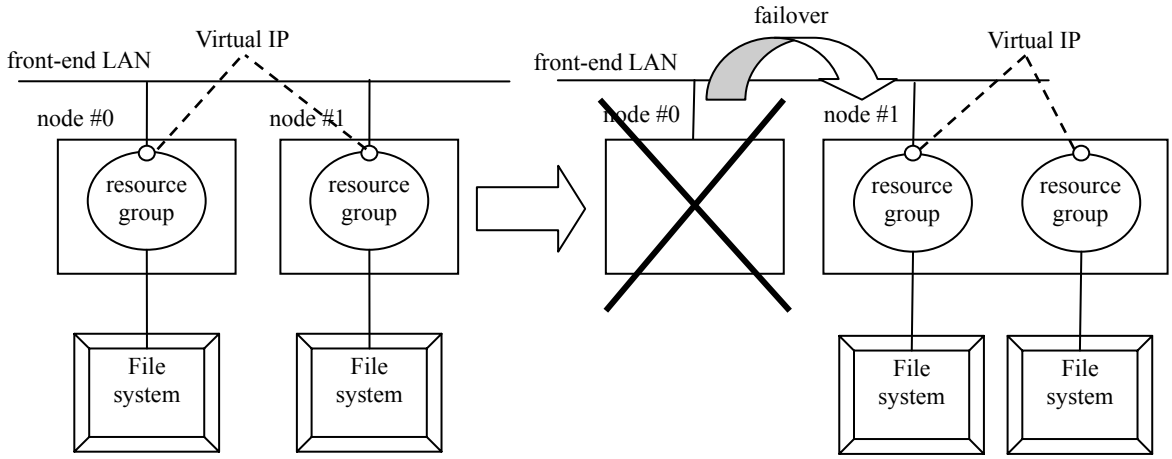


Figure 3.1.5-2 Imaginary figure of the Resource Group Failover

Copyright © 2010, 2012, Hitachi, Ltd.

3.1.6 Operating specifications of cache backup function

Cache backup function is a function that protect write cache on a RAID board.

NOTE:
- Only CR220SM and D51B-2U supports this function.
- When using cache backup function, the write policy to be set to “Write Back.”
- Some data written into the disk, such as disk cache and data on the internal drive cache, cannot be backed up by this function. Since the data described above can be lost at the time of an accidental power failure, system protection measures from accidental power failure should be separately considered.

(1) Operating specifications
- At the time of power failure, the cache backup module will continue to feed power for approximately 20 seconds. Meanwhile the data stored in the cache is written to the Flash ROM.
- The data written to the Flash ROM remains even after power feeding is finished. The data is written to the disk when the power feeding is restored.
- Recharge of the cache backup module finishes in a few seconds.
- Self-diagnosis is performed automatically during system start-up (up to 150 seconds) and when 30 days have elapsed from the last self-diagnosis (about 5 minutes.)

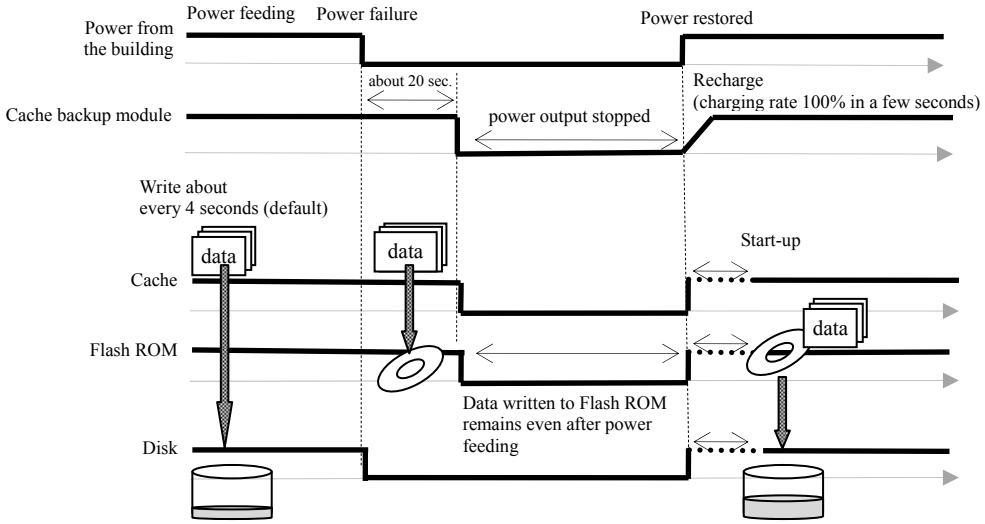


Figure 3.1.6-1 Data Sequence Diagram from Power Failure to Power Restoration

(2) Forced change of write policy
When it is impossible to protect the write cache, the write policy will be changed from “Write Back” to “Write Through” automatically.
Specifically, when a failure is detected in the cache backup module during self-diagnosis, the write policy will be changed to “Write Through” automatically.

Copyright © 2012, 2016, Hitachi, Ltd.

3.2 Specifications for Operations When a System Fails

3.2.1 Failures in the HDI system

Some parts on HDI nodes are configured redundantly and a node does not stop even if a part fails.

In addition, some parts can be replaced without stopping a node.

Whether a replaceable part is configured redundantly and whether such part can be replaced online is shown in Table 3.2.1-1 for the cluster configuration, and Table 3.2.1-2 for the single node configuration. Shaded parts cause a node down if they fail.

Table 3.2.1-1 Redundancy/Online Replacement Availability of Replaceable Parts (in the cluster configuration)

No.	Replaceable Parts	Redundancy	Online Replacement Availability
1	Memory	No	Not possible
2	Fibre Channel card	No	Not possible
3	LAN card	No	Not possible
4	Power unit	Yes (Two units)	If a power unit fails: Possible
			If two power units fail: Not possible
5	RAID controller	No	Not possible
6	Internal Drive	Yes (Two Drives (RAID1))	If a drive fails: Possible
			If two drives fail: Not possible
7	Fan unit	Yes (*3)	Not possible
8	BMC	No	Not possible
9	DVD drive	No	Not possible
10	Motherboard	No	Not possible
11	FC cable	Yes (*3)	Possible
12	LAN cable	Yes (*1,*2)	Possible
13	Management LAN IP-SW	No	Possible

*1: Make the data LAN redundant by link concentration or others.
*2: The management LAN is not redundant.
*3: The number is subject to the configuration.

Copyright © 2010, 2016, Hitachi, Ltd.

Table 3.2.1-2 Redundancy/Online Replacement Availability of Replaceable Parts (in the single node configuration)

No.	Replaceable Parts	Redundancy	Online Replacement Availability
1	Memory	No	Not possible
2	Power unit	Yes (Two units) (*2)	If a power unit fails: Possible (*4)
			If two power units fail: Not possible
3	RAID controller	No	Not possible
4	Internal Drive	Yes (Two Drives (RAID1) or 4/8/14 Drives (RAID configuration of user data: RAID5/RAID6/ RAID10))	If one drive fails: Possible
			If two drives fail: Possible (*4)
5	Fan unit	Yes (*4)	Not possible
6	BMC	No	Not possible
7	DVD drive	No	Not possible
8	Motherboard	No	Not possible
9	LAN card	No (*3)	Not possible
10	LAN cable	Yes (*1)	Possible
11	Internal RAID Battery	No	Not possible
12	Fibre Channel card (*5)	No	Not possible
13	Fibre Channel cable (*5)	Yes	Possible

*1: In the Configuration using trunk 2 Data ports, front-end LAN interface can be redundant by Link aggregation, etc. In the Configuration using Management port, front-end LAN interface cannot be redundant.
*2: The number is different depending on the target model.
*3: Not exist depending on the target model.
*4: Redundant is not made depending on the target model. In such a case, replacement while the power is ON is not allowed.
*5: Exists only in the configuration that is connected with the disk array subsystem.

Copyright © 2011, 2016, Hitachi, Ltd.

3.2.2 Operation policy when a failure occurs

3.2.2.1 Operation policy when a failure occurs in the single node configuration

When a failure occurs in an HDI node, there are cases when the node operation is continuing or stopped.

(1) When the node on which a failure occurred is operating
The service continues on the node on which the failure occurred. The failure part can be replaced while running the node. However, the failure recovery operation must be done with the power supply off of the node on which the failure occurs depending on the part to be replaced.
In this case, the service is stopped until the failure recovery is completed.

(2) When a node on which a failure occurred stops
When a failure occurs, the service is stopped due to the node termination as until the failure recovery is completed.
In the failure that accompanying the data recovery when not connected to the disk array subsystem, it will be the whole data recovery (with RAID reconfiguration) from the initial installation of OS unlike the cluster configuration. Recovery from the user data individually is not executed.
However, in the configuration connected to the disk array subsystem, or in the case of CR220SM or D51B-2U, recovery of the OS data and the user data to be executed individually.
Refer to Theory "3.2.7 Restoration of Data in the node in the single node configuration" (THEO 03-0210) for more information.

(3) In case of the Configuration of the single node with spare for Cloud
When a failure occurred, the system administrator isolates the failure occurred Active node from the front-end LAN and switches over the waiting Standby node to the Active node to resume the service. On the newly switched Active node, restore the data which has been migrated to HCP.
However, a service may be continued without switching the node if a failure occurred to redundant part. In this case, a policy will be the same as (1) stated above. If the power needs to be switched off in the failure recovery process, contact the system administrator to confirm whether the node to continue the service needs to be switched.
Maintenance personnel needs to ask the system administrator to confirm the management IP address of the Standby node when performing the new installation and configuration after installation.
Building and configuring the faulty node as the Standby node need to be performed by the system administrator. For the work responsibilities of a system administrator and a maintenance personnel, refer to the Table 3.2.2.1-1.

Copyright © 2010, 2015, Hitachi, Ltd.

Figure 3.2.2.1-1 explains the overview of the work responsibilities of a system administrator and a maintenance personnel when a failure occurs on OS in the Configuration of the single node with spare for Cloud.

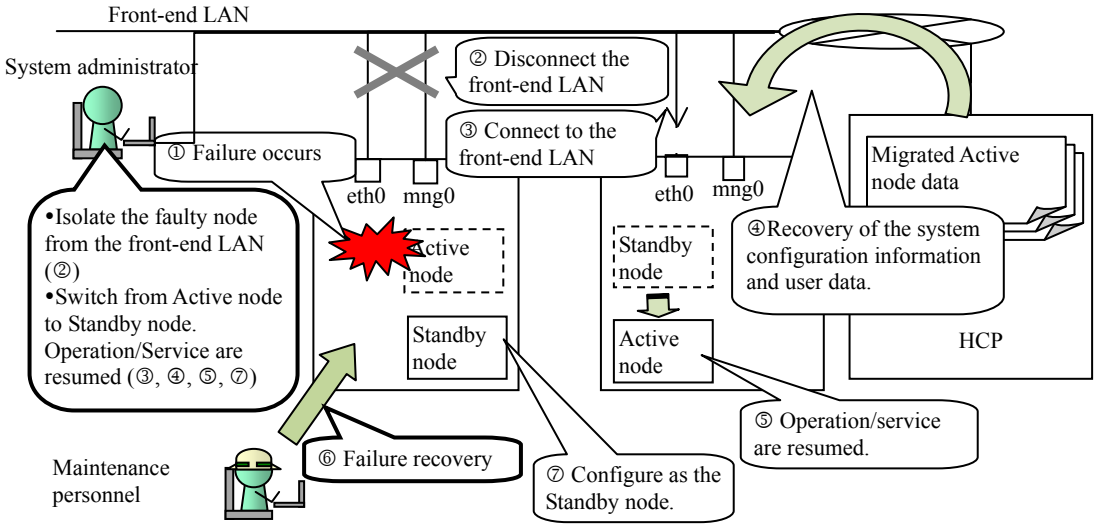


Figure 3.2.2.1-1 Overview of Operation when a Failure accompanying OS Error Occurs in the Configuration of the single node with spare for Cloud

Scenario of the failure recovery is as shown below.

Table 3.2.2.1-1 Scenario Examples of Failure Recovery in the Configuration of the single node with spare for Cloud

#	Working Description	Responsible person	Number corresponding to the Figure 3.2.2.1-1
1	Perform the failure recovery referring to the “Single Node Configuration Troubleshooting Guide” or “Message Reference”. If the failure cannot be solved or the action stated in the reference is “Contact the maintenance personnel” , contact the maintenance personnel.	System administrator	
2	Isolate the faulty node from the front-end LAN referring to the “Provisioning Guide” (*1).	System administrator	②
3	Connect the waiting Standby node to the front-end LAN as an Active node and restore the data from HCP to resume the operation. (*1) (*2).	System administrator	③④⑤
4	Failure determination of the faulty node.	Maintenance personnel	⑥
5	As the result of the failure determination, if the failure is the hardware induced failure, replace the defective parts.	Maintenance personnel	
6	As the result of the failure determination, if the failure is the hardware or software induced failure, newly install the hardware or software (including the configuration of the management IP (management IP address for the Standby node confirmed with the system administrator).	Maintenance personnel	
7	If the failure has recovered after newly installing the software or hardware, configure the IP address of the Standby and the system on GUI for the failure recovered node.	System administrator	⑦
8	If the failure has recovered without newly installing the hardware or software, connect the failure recovered node to the management console and get ready for activating as the Standby node using the singleinit command. (configure the IP address of the Standby node at the same time).	System administrator	
9	Connect to the network which has been isolated from the failure recovered node.	System administrator	

*1: If the service can continue as the failure is induced by such as redundant part failure, switching from Active node to Standby node is not required. However this switchover is performed at the system administrator`s discretion

*2: Steps after #4 shown above can be performed in parallel with #3.

Copyright © 2013, Hitachi, Ltd.

3.2.2.2 Operation policy when a failure occurs in the cluster configuration

When a single failure occurs in an HDI node, there are cases when the node operation is continuing or stopped.

(1) When the node on which a failure occurred is operating
The service continues on the node on which the failure occurred. The failure part can be replaced while running the node. However, the failure recovery operation must be done with the power supply off of the node on which the failure occurs depending on the part to be replaced.
In this case, the service is stopped until the failure recovery is completed.

(2) When a node on which a failure occurred stops
In the cluster configuration, if the node is stopped with the occurrence of a failure, perform failover the resource group with the following steps to continue the service in a remote node:
1. The failed node receives a reset command from the normally operating node.
2. A dump collection is started on the failed node.
3. The resource group on the failed node is failed over to the normally operating node.

Figure 3.2.2.2-1 and Figure 3.2.2.2-1-1 explains the overview of the failover operation.
For details about reset operations, refer to Theory "3.2.4 Notes on reset operations and operations when a dual failure occurs" (THEO 03-0150).
In addition, in case of a dual failure of the node of the HDI (including the overlap of one failure), the service might not be able to be continued.

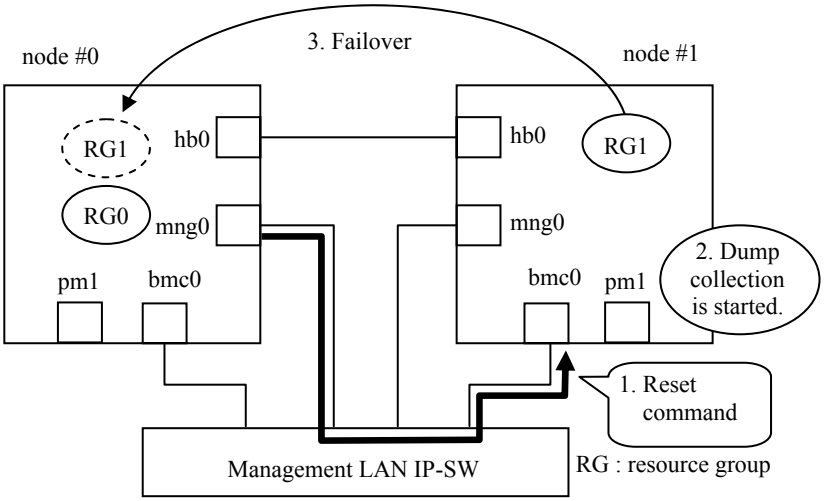


Figure 3.2.2.2-1 Overview of Failover Operation by the Auto Reset Function

Copyright © 2010, 2012, Hitachi, Ltd.

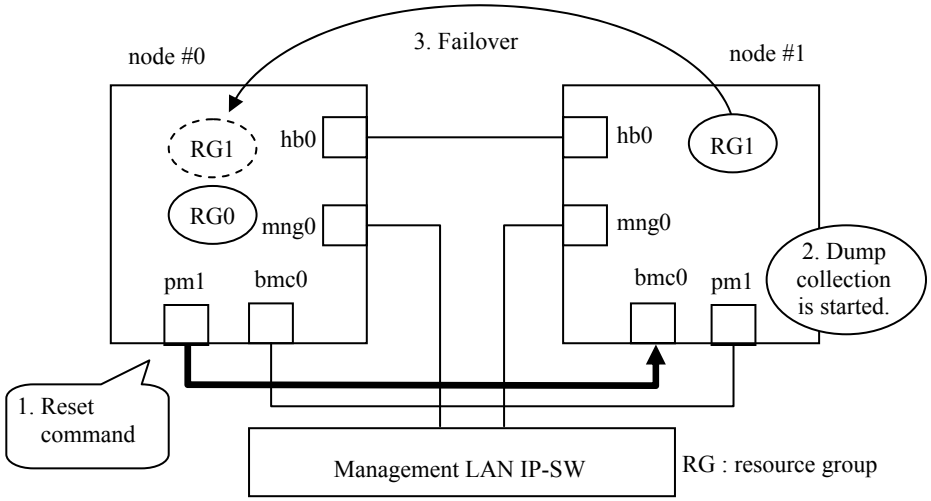


Figure 3.2.2.2-1-1 Overview of Failover Operation by the Auto Reset Function (BMC direct connection configuration)

Copyright © 2012, Hitachi, Ltd.

(3) In case a failure occurs in a Virtual Server
HDI does not support Virtual Server.

Copyright © 2010, 2011, Hitachi, Ltd.

3.2.3 Overview of failover operation

(1) Failover of HDI

In the cluster configuration, HDI consist of a cluster system configuration with two nodes. If a node stops, the other node takes over the processing of the failed node. Therefore, HDI can continue its operation.
This operation is called failover, and the operation for restoring the normal status is called failback.
The following subsections describe the read/write processing flow from when a failure occurs on the node 0 to when the processing is failed over to the node 1.

NOTE: Because mounting of "data of the past version directory" is not synchronized with start-up of the resource groups for the OS version 5.1.0-XX and later, the mounting of "data of the past version directory" on the migration target node to which a failover or failback has been performed might not be complete. In this case, the read/write operation for "data of the past version directory", mounting of which has not been complete, fails for a moment even if the failover or failback is complete.

(a) Read/write processing when an HDI node fails

If the node 0 side fails, the service of HDI is failed over to the node 1 side and continued, but the processing being executed at the time of failure occurrence is suspended. In that case, the read/write request from the client is required again after reconnection.
The operation is the same both at the time of Read and at the time of Write. The following figure shows an example at the time of Write.

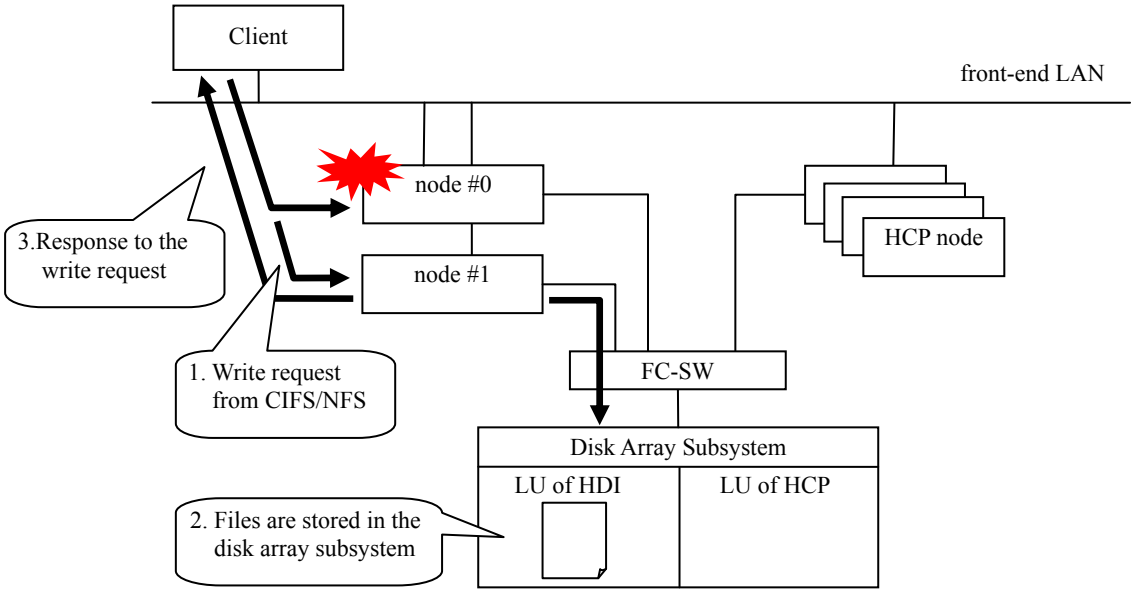
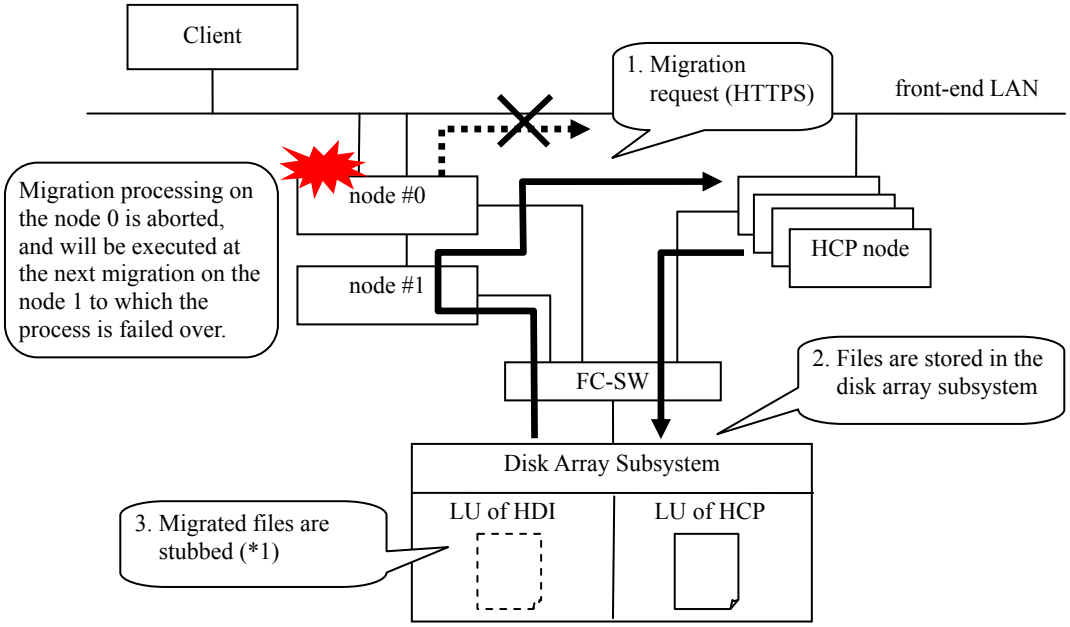


Figure 3.2.3-1 Write Processing When an HDI Node Fails

Copyright © 2010, 2014, Hitachi, Ltd.

(b) Migration processing when an HDI node fails
If the node 0 fails, the migration processing is performed on the node 1.
However, if the node 0 fails during the migration processing, the processing is aborted, and will be executed on the node 1 when the next migration is performed.



*1: When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default : 10%), the files are stubbed in chronological order of the last update dates and time.

Figure 3.2.3-2 Migration Processing When an HDI Node Fails

Copyright © 2010, 2011, Hitachi, Ltd.

(c) Recall processing when an HDI node fails
If the node 0 fails, the service of HDI is failed over to the node 1 and continued, but the processing being executed at the time of failure occurrence and the recall processing to be executed as an extension of the same are suspended, and an I/O error is returned. In that case, the read/write request from the client is required again after reconnection.
Both operations are the same at the time of reading and writing. The following figure shows an example at the time of reading.

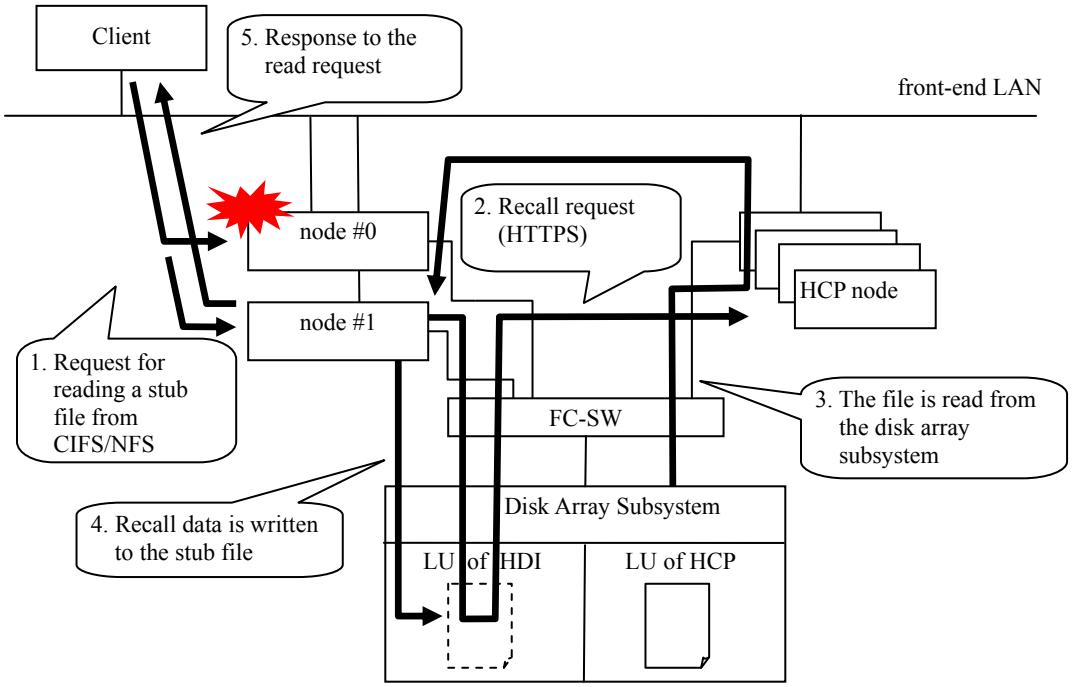
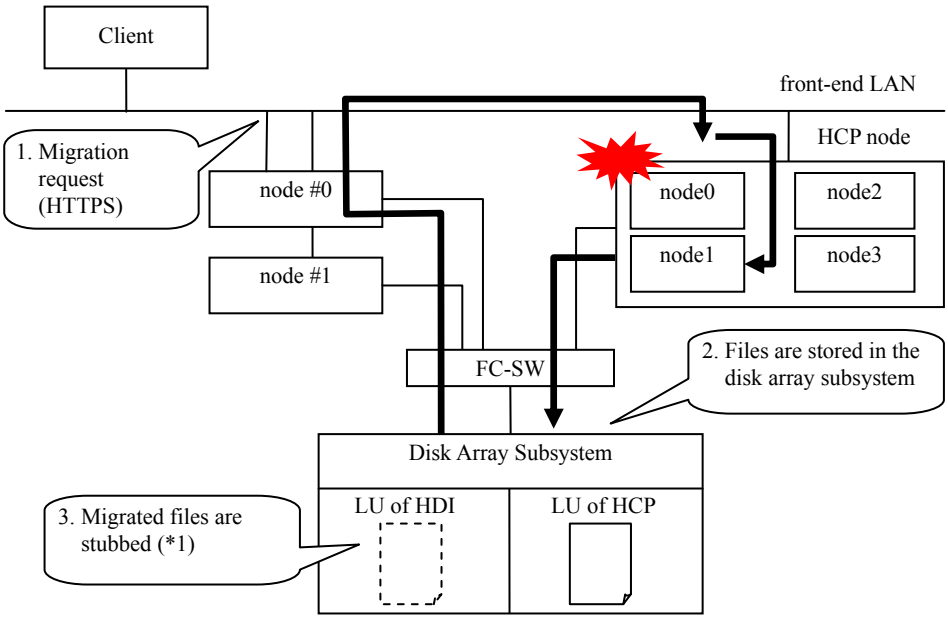


Figure 3.2.3-3 Recall Processing When an HDI Node Fails

Copyright © 2010, 2011, Hitachi, Ltd.

(2) Failover of HCP

(a) Migration processing when an HCP node fails
If an HCP node fails, a migration request is reissued to another HCP node, and then the migration processing is performed.



*1: When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default : 10%), the files are stubbed in chronological order of the last update dates and time.

Figure 3.2.3-4 Migration Processing When an HCP Node Fails

Copyright © 2010, 2011, Hitachi, Ltd.

(b) Recall processing when an HCP node fails
If an HDP node fails, a recall request is reissued to another HCP node, and then a recall processing is performed. Both operations are the same at the time of reading and writing. The following figure shows an example at the time of reading. If the response to the HCP is an I/O error due to the condition of the HCP, retry must be performed from the client after about 20 minutes.

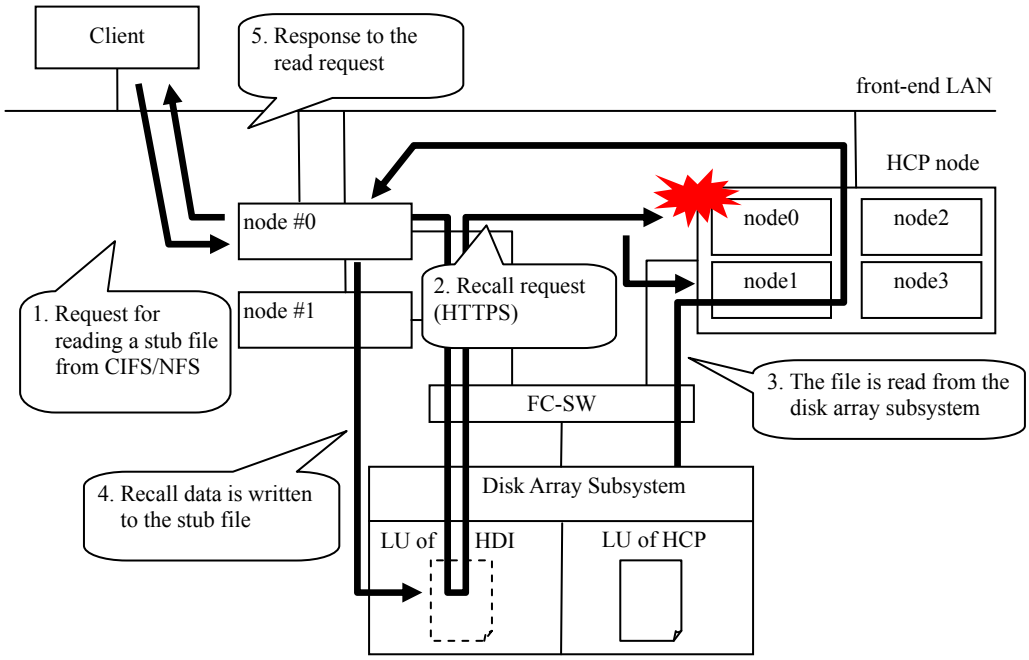


Figure 3.2.3-5 Recall Processing When an HCP Node Fails

Copyright © 2010, 2011, Hitachi, Ltd.

3.2.4 Notes on reset operations and operations when a dual failure occurs

(1) Reset path
Refer to (1-1) for the reset path in the BMC and Management SW connection configuration, and refer to (1-2) for the reset path in the BMC direct connection configuration.

(1-1) Reset path in the BMC and Management SW connection configuration
In the following description, the node 0 is described as a local system and the node 1 is described as a remote system.
In the node reset operation of HDI, if primary and secondary heartbeat cannot be confirmed between local and remote node, the OS automatically resets the node.
Automatic failover is performed the management port of the local node sends a reset command to the BMC port of the remote node.
Therefore, if a failure occurs in a path between the management port of the local node and the BMC port of the remote node, the reset operation fails and the automatic failover cannot be performed.

Note that when the heartbeat LAN operates normally and access from the management server to the management port is possible, manual failover can be performed.
If the management LAN IP-SW fails or the management ports of both nodes fail, automatic failover and manual failover cannot be performed because instructions from the system administrator cannot be delivered to both nodes.

However, if access from the maintenance PC to the maintenance port is possible and if permitted by the system administrator, the maintenance personnel can perform manual failover.

Figure 3.2.4-1 shows the reset path. In addition, Table 3.2.4-1 shows the failure locations that might cause reset failures. Note that failure locations shown in Table 3.2.4-1 are shown in numbers in Figure 3.2.4-1.

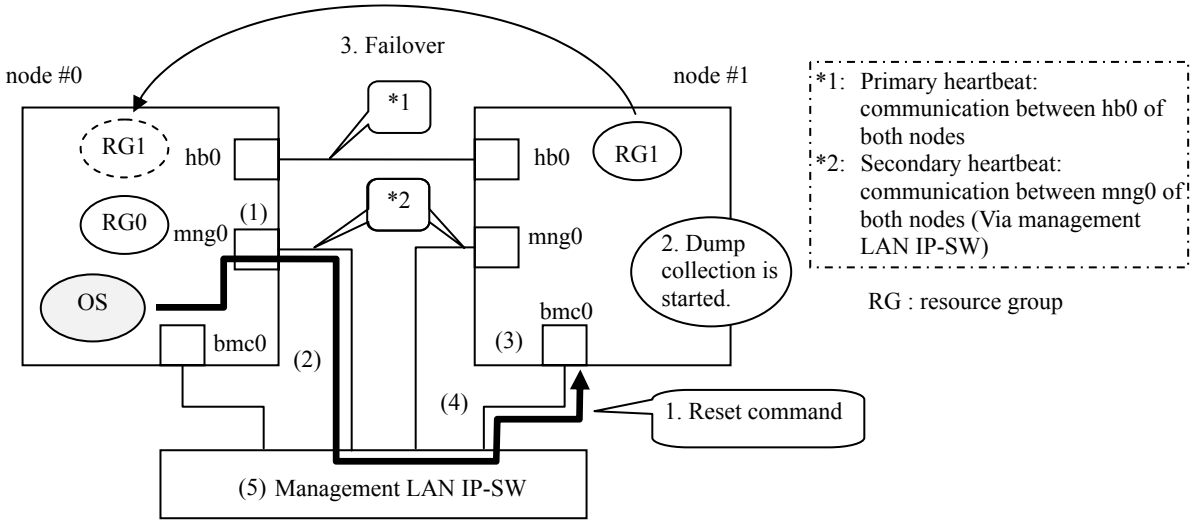


Figure 3.2.4-1 Reset Path

Table 3.2.4-1 Locations of Failures Causing Reset Failures

No.	Failure Location
(1)	Local management port
(2)	Local management port cable
(3)	Remote BMC port
(4)	Remote BMC port cable
(5)	Management LAN IP-SW (*1)

*1: Same in the case where the IP-SW owned by the customer is used.

Copyright © 2010, 2012, Hitachi, Ltd.

(1-2) Reset path in the BMC direct connection configuration

Automatic failover is performed the reset port of the local node sends a reset command to the BMC port of the remote node.
Therefore, if a failure occurs in a path between the reset port of the local node and the BMC port of the remote node, the reset operation fails and the automatic failover cannot be performed.

Note that when the heartbeat LAN operates normally and access from the management server to the management port is possible, manual failover can be performed.
If the management ports of both nodes fail, automatic failover and manual failover cannot be performed because instructions from the system administrator cannot be delivered to both nodes.

However, if access from the maintenance PC to the maintenance port is possible and if permitted by the system administrator, the maintenance personnel can perform manual failover.

Figure 3.2.4-1-1 shows the reset path. In addition, Table 3.2.4-1-1 shows the failure locations that might cause reset failures. Note that failure locations shown in Table 3.2.4-1-1 correspond to the numbers in Figure 3.2.4-1-1.

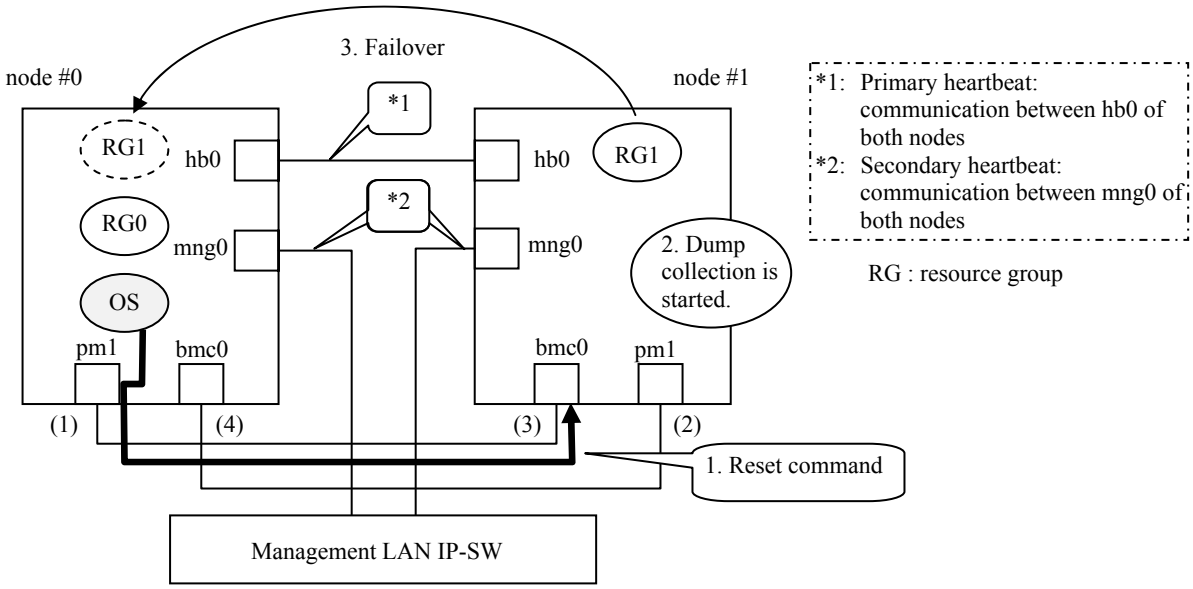


Figure 3.2.4-1-1 Reset Path (BMC direct connection configuration)

Table 3.2.4-1-1 Locations of Failures Causing Reset Failures

No.	Failure Location
(1)	Local reset port
(2)	Local reset port cable
(3)	Remote BMC port
(4)	Remote BMC port cable

Copyright © 2012, Hitachi, Ltd.

(2) Notes on operations when dual failures occur

Although it is detected that the dual failures occurrence and impossible communication of all the paths to confirm the heartbeat (the heartbeat ports or the management ports of the both nodes), there is a case that the resetting cannot be done. In such a case, the forced failover is executed automatically triggered by the failure of resetting. In case of link down in the management port of the forced failover target, the resource group for which failover was a performed change to [online/srmd executable error] and the services are stopped. If the restart operation is done to the node at this state, the resource groups of both nodes become [online/srmd executable error] and the entire services are stopped. Therefore, do not restart the node while forced failover is in operation.

During forced failover, the node suppresses LU accessing from the other side by using the reserve of fibre (SCSI command) to prevent the destruction of user data by the duplicated mounting of the file system. And it uses the release of fibre (SCSI command) to release the state of forced failover triggered by the recovery of the heartbeat communication.
SIM is output in each occasion. For the confirmation of SIM, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".
And for the details about measurement when each SIM is output, refer to "Troubleshooting 'Chapter 8 Messages' (TRBL 08-0000)".

The forced failover is executed when the following two SIMs are output.
Primary and Secondary heartbeats are disconnected
(KAQK39500-E OS error Detail=00 00 03 00 Level=00 Type=0D)
The remote resetting failed
(KAQK39507-E Reset to the other node was requested (result:failure, cause:XXXX, os status:XXXX)).

If the forced failover performed successfully, the SIM of "KAQG72026-E" is output.
After performing the forced failover, if the heartbeat communication recovers, the node that is performed the forced failover release the reservation, and resets the other side's node. At that time, the SIMs of "KAQK39507-E" and "KAQG72028-W" are output.

If it fails to get a reservation at the time of operating the forced failover, the SIM of "KAQG72027-E" is output. If the OSs of both nodes is running at the occasion of executing the forced failover, the both nodes try to execute the forced failover. In this case, when one node succeeded to get a reservation and execute the forced failover, the other node fails to get a reservation and outputs the SIM of "KAQG72027-E". If the SIM of "KAQG72027-E" is output on the both nodes, or if the other side of node of the node that the SIM of "KAQG72027-E" is output is stopped, getting a reservation fails by the cause of LU block. In that case, please contact to the technical support center. If the SIM of "KAQG72027-E" is output on one side node, but the SIM of "KAQG72026-E" is output on the other side node, there will be no problem because it succeeded the forced failover.

Copyright © 2010, 2017, Hitachi, Ltd.

If the heartbeat communication is recovered, but it failed to release the forced failover, the SIM of "KAQG72029-E" or "KAQG72030-E" is output.
At the time of releasing the forced failover, if a failure occurs on the path to be used for resetting, it fails the resetting to the other side node, and outputs the SIM of "KAQG72029-E". At that time, the other side node must be rebooted manually after removing the failure.
If it failed to release the reservation by the cause of LU block, the SIM of "KAQG72030-E" is output. In that case, refer to "Troubleshooting '5.3 Measures when Releasing the LU Access Protection Failed' (TRBL 05-0530)"
Table 3.2.4-2 shows examples of a failure that performs forced failover.

Table 3.2.4-2 Examples of A Failure that Performs Forced Failover

No.	Summary of failure	Failure example	
		node0	node1
1	Unable to access BMC + Node down	BMC failure + Node failure	Normal
2		Power supply dual failure	Normal
3	Failure in the reset path + Node down	Node down	Normal (Communication failed due to Management LAN IP-SW failure)
4		Node down	Management port failure
5		Node down	Reset port failure (in the BMC direct connection configuration)

*: In this example, the forced failover is performed on the side of node1.

Copyright © 2010, 2012, Hitachi, Ltd.

An example of performing the forced failover is shown below.

(a) This side node failure + this side BMC failure
If a BMC failure and another failure (such as memory failure) that stops a node occur almost at the same time, the resetting operation fails because it cannot be accessed to BMC.
And then, the forced failover is executed.

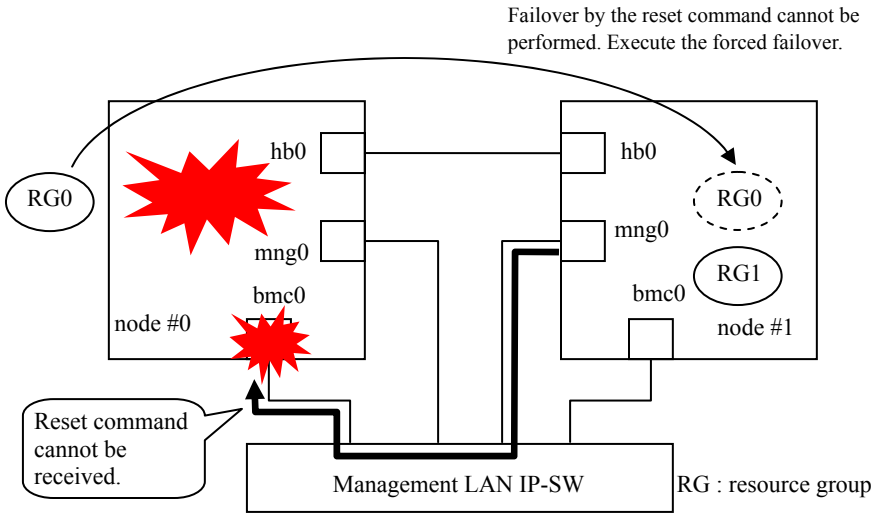


Figure 3.2.4-2 This side Node Failure + This side BMC Failure

(b) Power supply dual failure on the local node
If a power supply dual failure occurs, no power is supplied to the nodes.
Because of this, no heartbeat can be confirmed, and the normal node issues a reset command, but the reset operation fails because the power is not supplied to the BMC port of the failed node.
And then, the forced failover is executed.

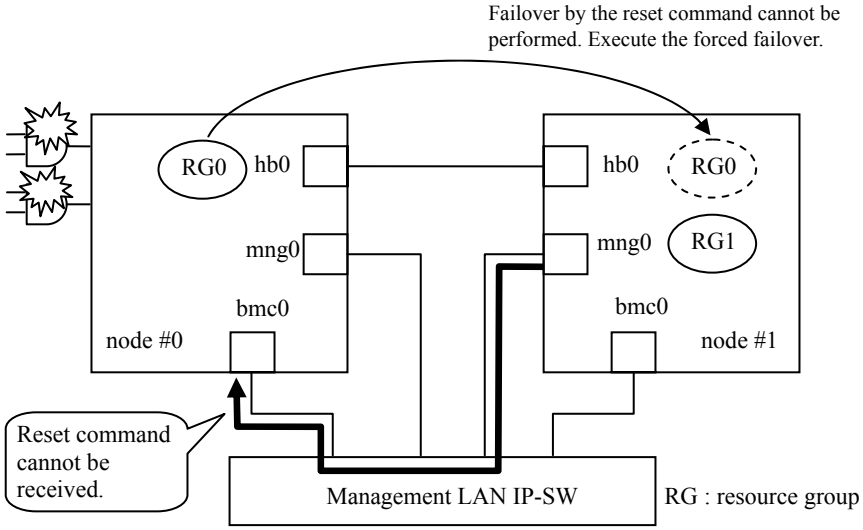


Figure 3.2.4-3 Power Supply Dual Failure on the Local Node

Copyright © 2010, 2011, Hitachi, Ltd.

3.2.5 Communication failure with HCP in the configuration of HDI for Cloud

In the configuration of HDI for Cloud, the Read/Write request from a client could fail because the communication is disconnected in a way of communication between HDI and HCP via WAN.

- The failure is not notified to Hi-Track/SNMP because it is not the failure of HDI itself.
- It responds I/O error for the client.
- When a client monitors HDI by introducing SNMP manager, the occurrence of a failure is reported to SNMP manager by SNMP Trap.

Figure 3.2.5-1 shows the recall operation when the WAN failure occurs as an example.

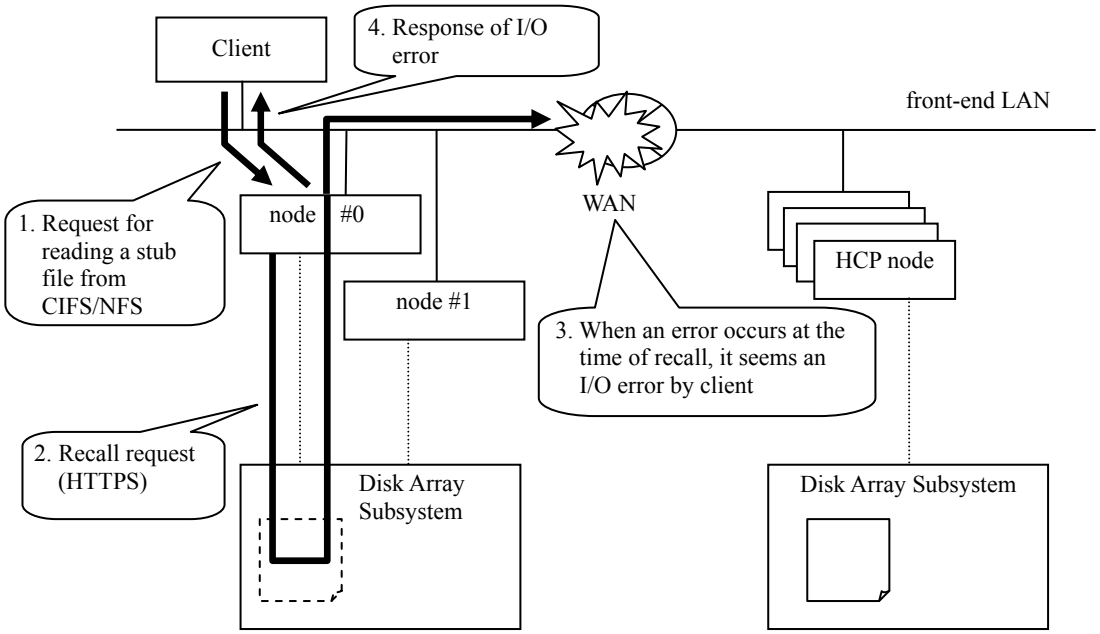


Figure 3.2.5-1 Operation When the WAN Failure Occurs in the configuration of HDI for Cloud (at the time of recall)

Copyright © 2010, 2012, Hitachi, Ltd.

If Read/Write from the client fails due to an I/O error, the client retries after 20 minutes or more elapses after the I/O error occurrence, and checks whether Read/Write is possible.
In the case where the node of HCP failed, the communication may be resumed by retrying from the client.
However, in the case where the communication pathway fails, the communication may not be resumed by retrying.

After an I/O error occurred by Read/Write from the client, even if you retry after 20 minutes or more elapsed but an I/O error still occurs, the system administrator performs determination with the following procedure.
Table 3.2.5-1 shows the procedure in the cluster configuration and Table 3.2.5-2 shows the procedure in the single node configuration.
Note that the maintenance personnel work is limited to, when em_alertfile indicate the error other than HCP error and network error at #3 or when it turns out that a failure has occurred in the node side of HDI at #4 in the cluster configuration, and when em_alertfile indicate the error other than HCP error and network error at #3, when the communication cannot be done with BMC at #4, when OS is running or a problem occurred in the lamp of the chassis at #5, or when I/O cannot be confirmed at #6 in the single node configuration. In that case, handle it in reference to the “Troubleshooting” in the Maintenance Manual.

Table 3.2.5-1 Procedure for System Administrator When the I/O Error Occurs in the cluster configuration

#	Procedure	Correspondence
1	Ask the client to retry the operation after waiting 20 min. or more.	•In case the communication is resumed → No measurement is required. •In case the I/O error occurs again → Proceed to #2.
2	Check the HCP connection status (hcpaccesstest) and the setting (archcpget)	• Access to HCP is possible → Proceed to #3. • Access to HCP is not possible → Confirm the HCP setting (archcpget) and, if the setting is not correct, perform the setting again by the archcpset command and proceed to #3.
3	Check the system message file (em_alertfile)	• In case of receiving the error status from HCP → The error status was received from HCP. Contact the HCP site for the recovery time of HCP. • In case of network system failure code → Failure between network including WAN and HCP Notify the HCP administrator that the access failure occurred in the access to HCP, and proceed to #4. • Cases other than the above → Call the maintenance personnel.
4	Check the status of the hardware and the cluster	• In case there is a failure in the front-end LAN (or other hardware) of the HDI node → Call the maintenance personnel. • When there is no failure in the front-end LAN of the HDI node → Proceed to #5.
5	Checking the status of NAT, front-end LAN-SW, DNS server and others by SNMP and others	• When there is an error in the status of NAT, front-end LAN-SW, DNS server and others → Try to recover NAT, front-end LAN-SW, DNS server and others. • When there is no error in the status of NAT, front-end LAN-SW and others → It may be a failure of WAN and later. Proceed to #6.
6	Contacting for the HCP condition of the HCP site	• When HCP is stopped (including error) → Contact the recovery time of HCP. • When HCP is not stopped (including the case where it is failed over and recovered) → This is a network failure. Contact the maintenance personnel of the WAN service vender.

Copyright © 2010, 2012, Hitachi, Ltd.

Table 3.2.5-2 Procedure for System Administrator When the I /O Error Occurs in the single node configuration (1/2)

#	Procedure	Correspondence
1	Ask the client to retry the operation after waiting 20 min. or more.	•In case the communication is resumed → No measurement is required. •In case the I/O error occurs again → Proceed to #2.
2	Check the HCP connection status and the setting	• Access to HCP is possible → Proceed to #3. • Access to HCP is not possible → Confirm the HCP setting by executing the CLI command published to the system administrator and, if the setting is not correct, perform the setting again and proceed to #3.
3	Check the system message file (em_alertfile)	• In case of receiving the error status from HCP → The error status was received from HCP. Contact the HCP site for the recovery time of HCP. • In case of network system failure code → Failure between network including WAN and HCP. Notify the HCP administrator that the access failure occurred in the access to HCP, and proceed to #7. • If the system message file (em_alertfile) cannot be confirmed → Check the status of network and environment server. If there is no problem, proceed to #4. • Cases other than the above → Execute troubleshooting of the trouble information confirmed by the system message file (em_alertfile) and, if the trouble cannot be recovered, call the maintenance personnel.
4	Checking if the communication is available with BMC (Communication checking by ping)	• In the case of communication is available with BMC → Proceed to #5. • In the case of communication is not available with BMC → If there is no problem found on the setting contents of the PC to be connected (such as IP address), call the maintenance personnel.
5	Checking if the OS is running (Checking from the remote console by connecting BMC)	• If the OS is running → Call the maintenance personnel. • If it cannot be confirmed that the OS is running → Check the lamp of the chassis. If there is a problem, call the maintenance personnel. If there is no problem, perform the OS reboot by NMI issue operation with the manually collecting a dump, and proceed to #6. Refer to Installation "2.1.3.2 OS reboot of a node by NMI issue operation (single node configuration only)" (INST 02-0140) for NMI issue operation.

Copyright © 2010, 2014, Hitachi, Ltd.

Table 3.2.5-2 Procedure for System Administrator When the I /O Error Occurs in the single node configuration (2/2)

#	Procedure	Correspondence
6	Checking if the OS is started by the rebooting process with the manual dump	• If the OS is stared, and I/O of end user can be resumed. → No measurement is required (the maintenance personnel will collect the failure information later). • Cases other than the above → Call the maintenance personnel.
7	Check the hardware status	• If there is a problem in the hardware of the HDI node → Call the maintenance personnel. • If no problem is found in the hardware of the HDI node → Proceed to #8.
8	Checking the status of NAT, front-end LAN-SW, DNS server and others by SNMP and others	• When there is an error in the status of NAT, front-end LAN-SW, DNS server and others → Try to recover NAT, front-end LAN-SW, DNS server and others. • When there is no error in the status of NAT, front-end LAN-SW and others → It may be a failure of WAN and later. Proceed to #9.
9	Contacting for the HCP condition of the HCP site	• When HCP is stopped (including error) → Contact the recovery time of HCP. • When HCP is not stopped (including the case where it is failed over and recovered) → This is a network failure. Contact the maintenance personnel of the WAN service vender.

Copyright © 2011, 2012, Hitachi, Ltd.

3.2.6 Restoration of File System in the migration operation in the cluster configuration

If the data is lost due to HDI failure, the file system can be restored by using he data migrated to the HCP.

However, the changes of the file after the last migration that was performed before the occurrence of the failure cannot be restored.

The following shows the procedures for restoring data in the file system as a case of a RAID group failure.

Note that the maintenance personnel work is only the failure recovery of procedure #1 in Table 3.2.6-1 Procedure for Restoring File System, and procedure #2 to #4 are the system administrator's work.

Table 3.2.6-1 Procedures for Restoring File System

#	Procedure	Overview	Worker
1	Recovering failures	Perform the recovery procedure of the RAID group failure.	Maintenance personnel
2	Creating a file system to be restored in HDI	Create a file system to restore the following conditions. • The File system capacity must be the same or more as the one before the restoration. • Enable WORM if WORM was enabled in the file system where the failure occurred. • Specify the same ACL type as the file system where the failure occurred. • The file system must be mounted in the readable and writable status.	System administrator
3	Executing file system restoration	Execute the CLI command that is open to the system administrator and execute restoration of the file system whose data was migrated to the HCP.	System administrator
4	Executing the consistency check of the file that restored	Execute CLI command that is open to the system administrator, and then check if there is no inconsistency in the file configuration between HDI and HCP after the restoration.	System administrator

Copyright © 2010, 2011, Hitachi, Ltd.

3.2.7 Restoration of Data in the node in the single node configuration

In the single node configuration, if the data is lost due to HDI failure, the data can be restored from the backup information after installing the OS initially.

The configuration using Management port sets the management port shortly after the new installation and recover the data using the management port.
The configuration using trunk 2 Data ports change the setting of cable connection and the IP-SW which the customer configures to recover the data using the management port.

In the HDI for Cloud configuration, the entire data in the node can be restored at one time because the backup information of HCP stores backup data of OS area and user area.

In the single node configuration which is connected to the disk array subsystem, if the data is lost due to HDI failure, the procedure for restoring data in the node differs depending on whether the failure occurred on the node or on the disk array subsystem.
If the failure occurred on the node, restore the OS area after installing the OS initially because the user data on the disk array subsystem is not lost.
If the failure occurred on the disk array subsystem, execute the same recovery procedure as in the case the disk array subsystem is not connected after restoring the disk array subsystems

In the case OS area and user area are divided (CR220SM or D51B-2U), execute a different procedure without a new OS installation.

The following shows the procedures for restoring data in the node.

Note that the procedures to the state of restoration in the single node configuration is different by its configuration as shown in Table 3.2.7-1 and Table 3.2.7-2.

Table 3.2.7-1 Procedures for restoring data in the node in the configuration using management port

#	Contents	Worker
1	Execute the initial OS installation (with RAID reconfiguration) (*1) (*2)	Maintenance personnel
2	Execute setup after installation is complete.	Maintenance personnel
3	Execute the restoration of the system LU (including user data) (*3)	System administrator
4	Confirm that no error message related to the file system or the file sharing is output	System administrator
5	In the HDI for Cloud configuration, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by executing the CLI command open to the system administrator.	System administrator
6	Execute the I/O confirmation for the system	System administrator

*1: All data within the node will be initialized.
*2: In the configuration connected to the disk array subsystem (except for CR220SM) and the OS version of the installation media is 4.0.0-XX or later, execute the installation without user data initialization.
*3: Although the data in the OS area/user area can be restored at one time in HDI for Cloud, in the Basic Configuration, restoration of the data in the OS area/user area is need to be executed individually and also deleting and re-creating the file system are required before restoring the data in the user area.

Copyright © 2012, 2015, Hitachi, Ltd.

Table 3.2.7-2 Procedures for restoring data in the node in the configuration using trunk 2 Data ports

#	Selection	Contents	Worker
1	Common	Ask the system administrator for a free port of the IP-SW which the customer configures.	Maintenance personnel
2	Common	•If a free port of IP-SW is available, connect the LAN cable and change the settings. Execute the procedure “A” shown in the Selection line. •If a free port of IP-SW is not available, ask the system administrator to change the IP-SW settings (disable settings of VLAN/Link aggregation). Execute the procedure ”B” shown in the Selection line (*1)	Maintenance personnel
3	A	Connect the free port confirmed with the system administrator and management port of the node by a LAN cable.	Maintenance personnel
	B	Disable settings of VLAN/Link aggregation of the port which the node and IP-SW are connecting. (Ask the system administrator to leave a note of the settings before changing the settings)	System administrator
		Remove a LAN cable from a node data port connecting to the IP-SW port which setting was changed by the system administrator and reconnect to the management port.	Maintenance personnel
4	Common	Execute the initial OS installation (with RAID reconfiguration) (*2)	Maintenance personnel
5	Common	Execute setup after the installation is complete. (Set the IP address and the routing used for trunk 2 data ports in the front-end LAN to the Management port IP address. Ask the system administrator about the IP address and the routing for trunk 2 data ports in the front-end LAN.)	Maintenance personnel
6	Common	Execute the restoration of the system LU (including user data) (*3) (*4)	System administrator
7	A	Remove the LAN cable between IP-SW of front-end LAN and the management port that was connected at sequence #3-A of the node.	Maintenance personnel
	B	Put the LAN cable which was reconnected at the above step #3-B back to the original data port.	Maintenance personnel
		Restore the IP-SW settings changed at sequence #3-B of the node (VLAN/Link aggregation).	System administrator
8	Common	Confirm that no error message related to the file system or the file sharing is output	System administrator
9	Common	In the HDI for Cloud configuration, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by using the CLI command open to the system administrator.	System administrator
10	Common	Execute the I/O confirmation for the system	System administrator

*1: Since the configuration using trunk 2 Data ports keep a free port, this procedure is not executed normally.
*2: All data within the node will be initialized.
*3: Although the data in the OS area/user area can be restored at one time in HDI for Cloud, restoration of the data in the OS area/user area is need to be executed individually and also deleting and re-creating the file system are required before restoring the data in the user area.
*4: KAQG81003-W will be output after rebooting at the time of the OS data recovery. However no particular action is required. Continue the recovery procedure.

Table 3.2.7-3 Procedures for restoring data in the node in the configuration using management port when connected to the disk array subsystem

#	Contents	Worker
1	Execute the initial OS installation (without RAID reconfiguration) (*1)	Maintenance personnel
2	Execute setup after installation is complete	Maintenance personnel
3	Execute the restoration of the OS area (recovery of user data is not required)	System administrator
4	Execute the I/O confirmation for the system	System administrator

*1: Because there is no failure in the user data on the disk array subsystem.

Copyright © 2012, 2013, Hitachi, Ltd.

Table 3.2.7-4 Procedures for restoring data in the node in the configuration using trunk 2 Data ports when connected to the disk array subsystem

#	Selection	Contents	Worker
1	Common	Ask the system administrator for a free port of the IP-SW which the customer configures.	Maintenance personnel
2	Common	•If a free port of IP-SW is available, connect the LAN cable and change the settings. Execute the procedure “A” shown in the Selection line. •If a free port of IP-SW is not available, ask the system administrator to change the IP-SW settings (disable settings of VLAN/Link aggregation). Execute the procedure”B” shown in the Selection line (*1).	Maintenance personnel
3	A	Connect the free port confirmed with the system administrator and management port of the node by a LAN cable.	Maintenance personnel
	B	Disable settings of VLAN/Link aggregation of the port which the node and IP-SW are connecting. (Ask the system administrator to leave a note of the settings before changing the settings)	System administrator
		If the OS version is 4.0.1-XX or earlier, remove a LAN cable from a node data port connecting to the IP-SW port which setting was changed by the system administrator and reconnect to the management port.	Maintenance personnel
4	Common	Execute the initial OS installation (without RAID reconfiguration) (*2)	Maintenance personnel
5	Common	Execute setup after the installation is complete. (Set the IP address and the routing used for trunk 2 data ports in the front-end LAN to the Management port IP address. Ask the system administrator about the IP address and the routing for trunk 2 data ports in the front-end LAN.)	Maintenance personnel
6	Common	Execute the restoration of the OS area (recovery of user data is not required) (*3)	System administrator
7	A	Remove the LAN cable between IP-SW of front-end LAN and the management port that was connected at sequence #3-A of the node.	Maintenance personnel
	B	Put the LAN cable which was reconnected at the above step #3-B back to the original data port.	Maintenance personnel
		Restore the IP-SW settings changed at sequence #3-B of the node (VLAN/Link aggregation).	System administrator
8	Common	Execute the I/O confirmation for the system	System administrator

*1: Since the configuration using trunk 2 Data ports keep a vacant port, this procedure is not executed normally.
*2: Because there is no failure in the user data on the disk array subsystem.
*3: KAQG81003-W will be output after rebooting at the time of the OS data recovery. However no particular action is required. Continue the recovery procedure.

Copyright © 2012, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2013, Hitachi, Ltd.

Chapter 4 Maintenance Actions

4.1 Support Ranges

The following figures show the ranges of components supported by HDI.

Figure 4.1-1 shows the support range for HDI in the configuration of HDI for HCP (cluster configuration).
Figure 4.1-2 shows the support range for HDI in the configuration of HDI for Cloud (cluster configuration).
Figure 4.1-3 shows the support range for HDI in the configuration of HDI for HCP (single node configuration).
Figure 4.1-4 shows the support range for HDI in the configuration of HDI for Cloud (single node configuration).

The following figures are examples when the management LAN IP-SW provided by (HDS) is introduced.
If a management LAN IP-SW provided by the customer is introduced, all the devices connected to the management LAN IP-SW are supposed to be connected to the front-end IP-SW owned by the customer. In addition, since the maintenance IP-SW disappears, the maintenance personnel work by directly connecting the maintenance PC to each node.

Copyright © 2010, 2014, Hitachi, Ltd.

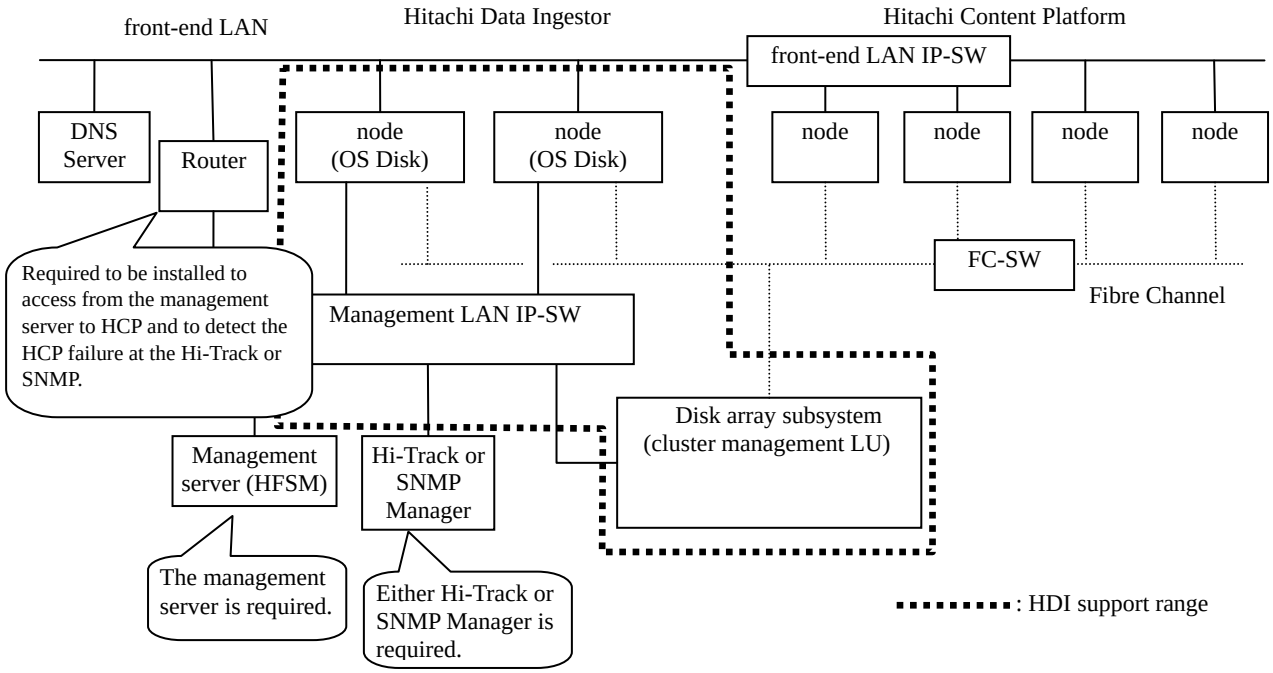


Figure 4.1-1 Support Range in the Configuration of HDI for HCP (Cluster configuration)

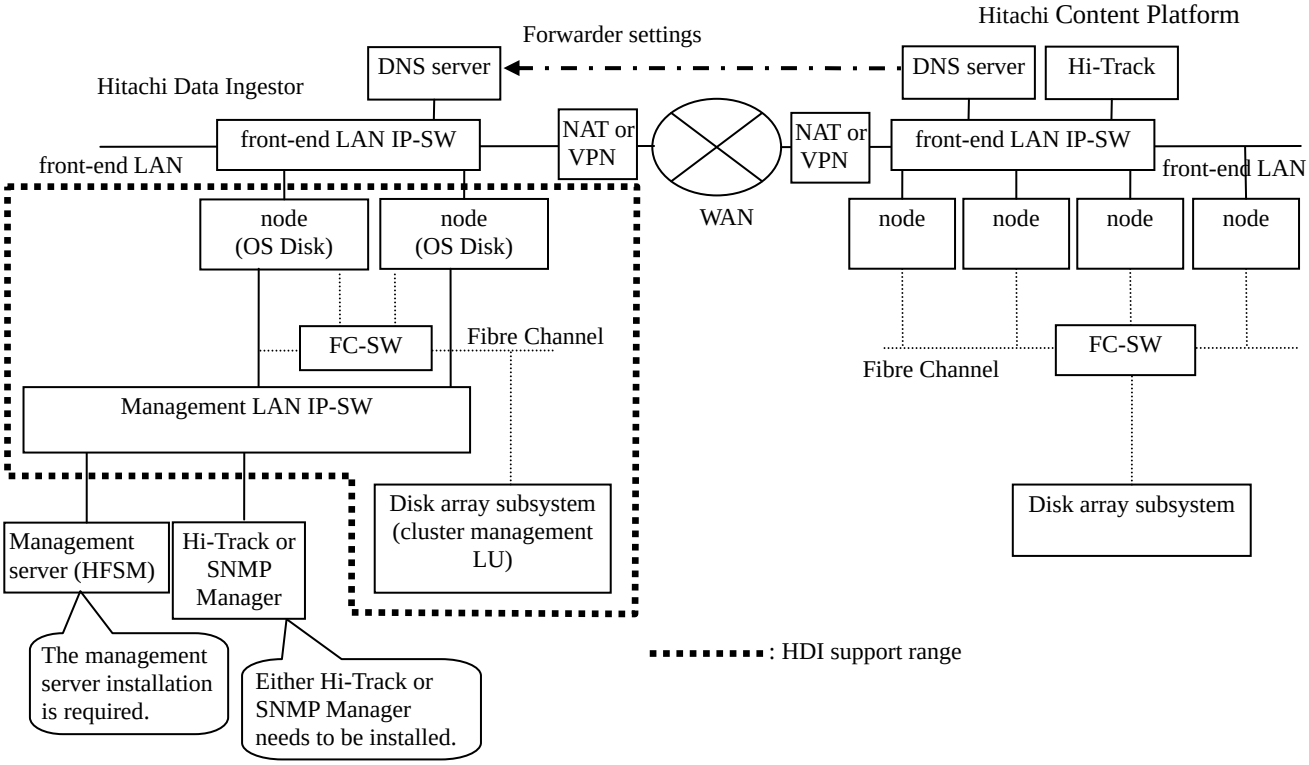


Figure 4.1-2 Support Range in the Configuration of HDI for Cloud (Cluster configuration)

Copyright © 2010, 2013, Hitachi, Ltd.

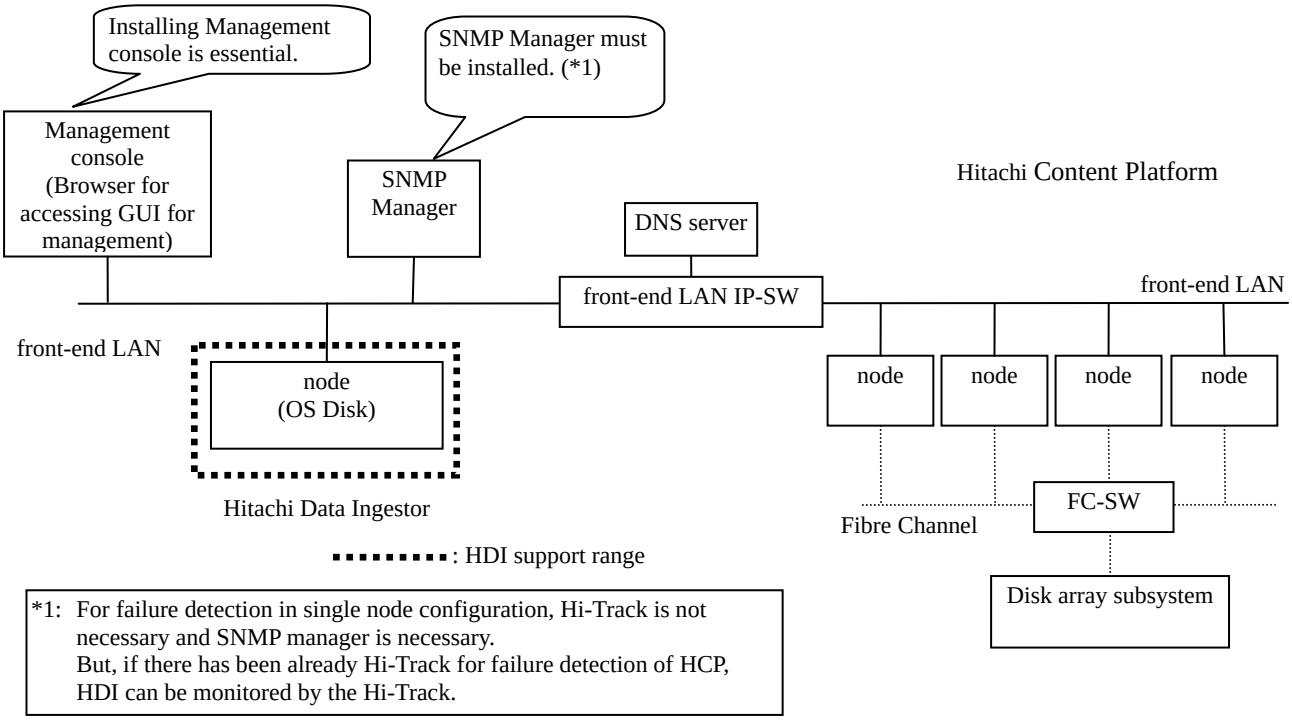


Figure 4.1-3 Support Range in the Configuration of HDI for HCP (Single node configuration)

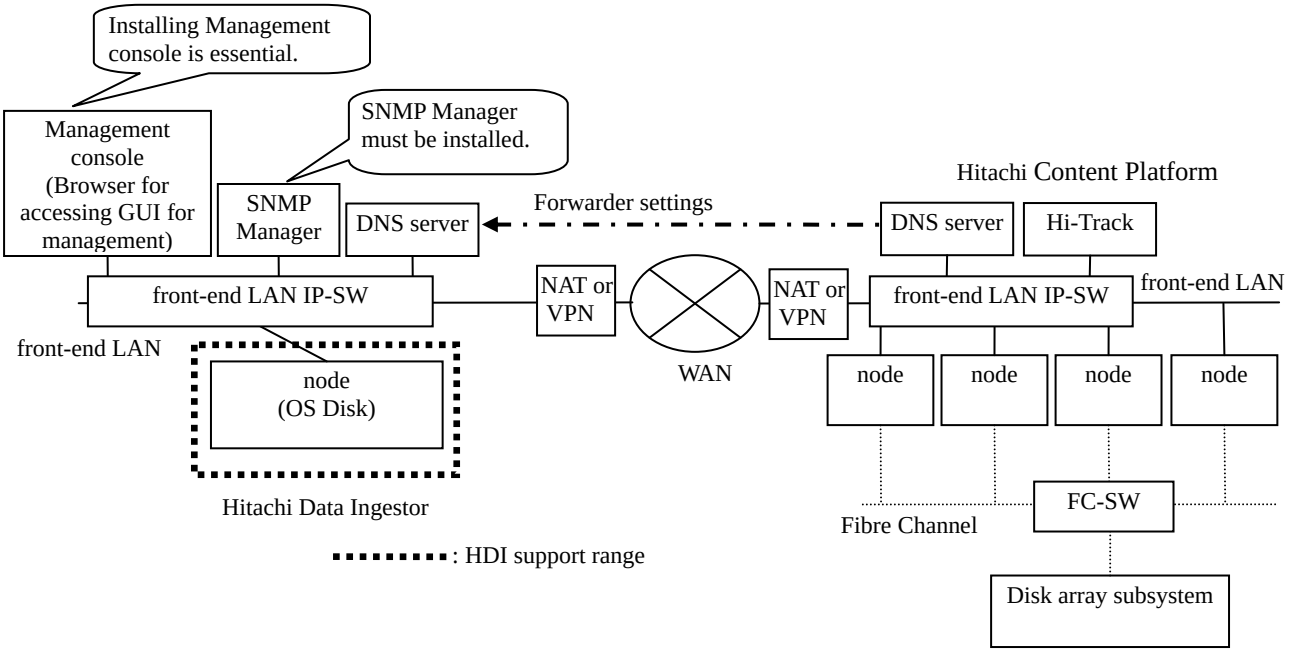


Figure 4.1-4 Support Range in the Configuration of HDI for Cloud (Single node configuration)

Note that the figure above shows the supported range in the single node configuration which is not connected to the disk array subsystem. If connected to the disk array subsystem, the disk array subsystem will be included in the supported range.

Copyright © 2010, 2012, Hitachi, Ltd.

4.2 Work that the Customer Performs

NOTE: This section describes information about the cluster configuration.

(1) Starting and terminating the service of a node

Starting or terminating the service of a node means starting or terminating the various services provided by the node, and is different from the starting or terminating of OS of the node. Because starting or terminating the services of a node is described in the user guide as starting or terminating of a node, be careful when you request the operation to the system administrator.

(2) Failover/failback methods and node service start/termination methods

There are automatic and manual methods for performing a failover.
When a failure occurred and the service cannot be continued, failover is performed automatically.
While in the normal operation, the system administrator can execute failover or failback manually by using HFSM.
The system administrator also can start or terminate the services of a node manually by using HFSM.
To start the services of a node, it should be done in the order of starting a node and then starting the services of the node, and to terminate the services of a node, it should be done in the order of terminating the services of a node and then terminating the node.

To terminate the node because the parts are required to be replaced when a failure occurred, the maintenance personnel can perform failover, failback, or starting or terminating of services of a node manually.
When a maintenance personnel performs these operations, get a permission from the system administrator, and check the status of the maintenance target node by referring to “Maintenance Tool ‘Chapter 3 Appendix A Cluster operations by the maintenance personnel’ (MNTT 03-0000)” before the operation.

Copyright © 2010, 2012, Hitachi, Ltd.

4.3 Maintenance Actions when Linking with HCP

4.3.1 Considerations in the normal operation

Before the HDI resource group is started, HCP must have been started. Before HCP is stopped, the HDI resource group must have been stopped.

If the HDI resource group is started when HCP has stopped, the migration or recall processing fails. Figures 4.3.1-1 and 4.3.1-2 show the schematic figures of the failures.

Note that, although these figures are based on the configuration of HDI for HCP and cluster configuration for explanation, the same logic also applies to the configuration of HDI for Cloud and single node configuration.

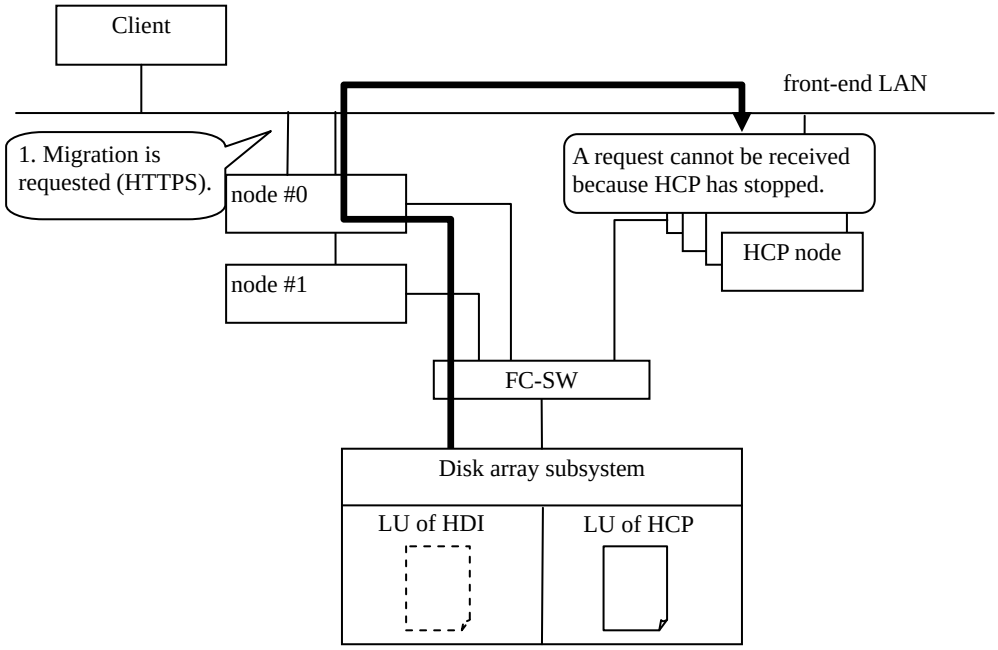


Figure 4.3.1-1 Migration Processing when HCP has Stopped

Copyright © 2010, 2011, Hitachi, Ltd.

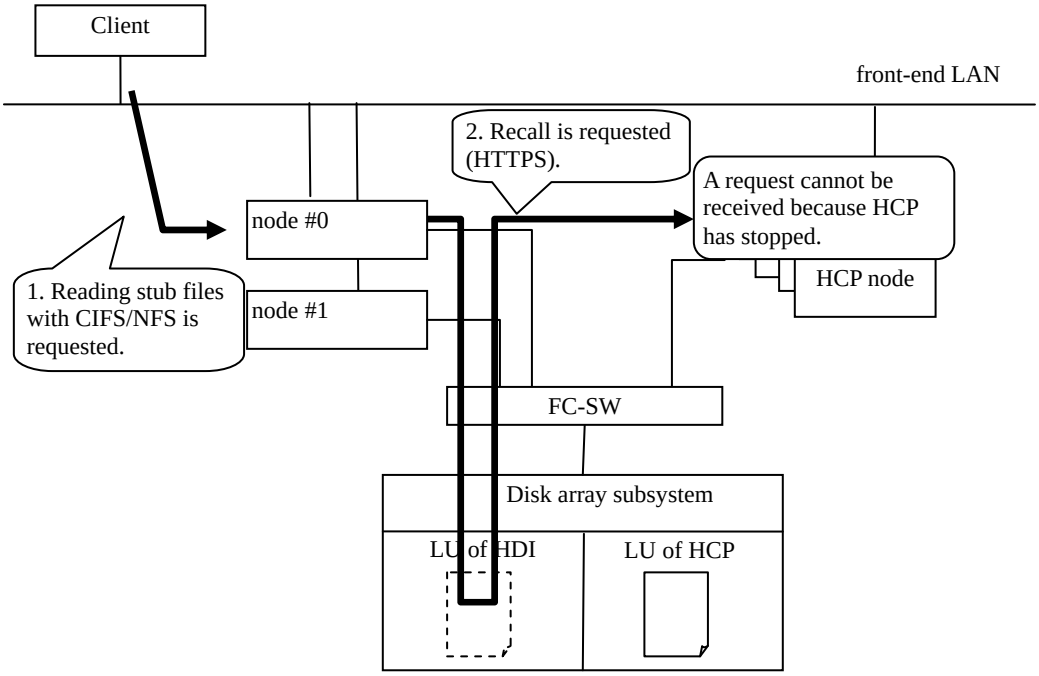


Figure 4.3.1-2 Recall Processing when HCP has Stopped

Copyright © 2010, 2012, Hitachi, Ltd.

4.3.2 Maintenance actions when a failure occurs

If a failure occurs, it is reported to the HDI or HCP according to the failed part.

Basically, maintenance is performed on the side to which a failure is reported. However, if a failure is reported to both sides of HDI and HCP, maintenance must be performed linking with both sides.

Table 4.3.2-1 shows the failure notices in each failed part in the cluster configuration, and Table 4.3.2-2 shows the failure notices in each failed part in the single node configuration.

Table 4.3.2-1 Failed parts and failure report destinations (In the cluster configuration)

#	Failed part	Failure notice
1	HDI node	A failure is reported to HDI.
2	Management LAN IP-SW (*1)	A failure is reported to HDI.
3	Disk array subsystem	• In the configuration of HDI for HCP, a failure is reported to both HDI and HCP. Maintenance must be performed linking with both the HDI and HCP sides. • In the configuration of HDI for Cloud, a disk array subsystem failure that occurs on the HDI side is reported to HDI, and a disk array subsystem failure that occurs on the HCP side is reported to HCP.
4	FC-SW (a failure is detected as an FC path failure)	• In the configuration of HDI for HCP, a failure is reported to both HDI and HCP. • In the configuration of HDI for Cloud, FC-SW at the HDI side reports a failure to the HDI side. An FC-SW failure that occurs on the HCP side is reported to HCP.
5	front-end LAN	• In the configuration of HDI for HCP, a failure is reported to both HDI and HCP. • In the configuration of HDI for Cloud, a front-end LAN failure that occurs on the HDI side is reported to HDI, and a front-end LAN failure that occurs on the HCP side is reported to HCP.
6	HCP node	The failure is reported to HCP. The failure is not reported to HDI.

*1: Even in case the management LAN IP-SW prepared by the customer is introduced, the management network (the management port or the BMC) notifies a failure to the HDI side as the conventional process.

Table 4.3.2-2 Failed parts and failure report destinations (In the single node configuration)

#	Failed part	Failure notice
1	HDI node	A failure is reported to HDI.
2	Disk array subsystem (*1)	• A failure that occurs on the HDI side is reported to HDI, and a failure that occurs on the HCP side is reported to HCP.
3	FC-SW (a failure is detected as an FC path failure)	In the configuration of HDI for Cloud, FC-SW at the HDI side reports a failure to the HDI side. An FC-SW failure that occurs on the HCP side is reported to HCP.
4	front-end LAN	• In the configuration of HDI for HCP, a failure is reported to both HDI and HCP. • In the configuration of HDI for Cloud, a front-end LAN failure that occurs on the HDI side is reported to HDI, and a front-end LAN failure that occurs on the HCP side is reported to HCP.
5	HCP node	A failure is reported to HCP. A failure is not reported to HDI.

*1: A failure will be reported only when the single node configuration connected to the disk array subsystem.

Copyright © 2010, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2014, Hitachi, Ltd.

Chapter 5 LAN Configuration Settings

This chapter describes the LAN interfaces and their settings for Hitachi Data Ingestor.

5.1 LAN Interface Setting Items

Table 5.1-1 shows the setting items that the maintenance personnel must specify correctly for using a LAN interfaces between a node and the device to be connected to the node.

Table 5.1-1 LAN Interface Setting Items

Port	IP address		Negotiation mode	MTU
	IPv4	IPv6		
Private Maintenance port	Y (essential)	Y	Auto Negotiation (fixed)	1500 (fixed)
Heartbeat port (*1) (set up by the administrator at the installation destination)	Y (essential)	N	100Base Full Duplex (fixed)	1500 (fixed)
Management port (*5)	Y (essential)	Y	Auto Negotiation (Default), 1000Base Full Duplex, 100Base Full Duplex (*4), 100Base Half Duplex (*4)	1500 (fixed)
BMC port	Y (essential)	N	Auto Negotiation (fixed)	1500 (fixed)
Data port (*2)(*5) (set up by the administrator at the installation destination)	Y	Y	Auto Negotiation (Default), 1000Base Full Duplex, 100Base Full Duplex (*4), 100Base Half Duplex (*4)	Variable (initial value: 1500)
Reset port (*1)(*3)	Y (essential)	N	Auto Negotiation (fixed)	1500 (fixed)

Legend:
Y (#1) : The setting must be specified on the node.
N : The setting need not be specified.

*1: It does not exist in the single node configuration.
*2: This is not used in the single node Configuration using Management port.
*3: This is used only in the BMC direct connection configuration. In the BMC direct connection configuration, reset port IP address is automatically set when BMC port IP address is set. In this case, set a BMC port IP address of which the network segment is different from the management port IP address.
*4: For the setting of Auto Negotiation in 100Base, in case that the OS version is 3.2.2-XX or earlier, it sets to “ON”. In case of 3.2.3-XX or later, and 4.1.0-01 or earlier, it sets to “OFF”. In case of 4.1.0-02 or later, you can select either “ON” or “OFF”.
*5: In the case of D51B-2U, the port of 10GbE can only set Auto Negotiation.

(a) LAN Interface settings
Specify the setting of each LAN interface. You can change the settings while the system is operating. For the setting and the confirmation, it uses the maintenance CLI. If you change the setting, obtain the setting information from the system administrator.

- For details about how to perform the Private Maintenance port settings, refer to “Maintenance Tool ‘2.41 Configuring a Private Maintenance LAN Port (pmctl)’ (MNTT 02-2370)”.
- For details about how to perform the Management port settings, refer to “Maintenance Tool ‘2.12 Setting the Management Port Information (ownmngifedit)’ (MNTT 02-0840)”.
- For details about how to perform the BMC port and the Reset port settings, refer to “Maintenance Tool ‘2.18 Setting BMC LAN Information (bmcctl)’ (MNTT 02-1210)”.

Copyright © 2010, 2015, Hitachi, Ltd.

(a-1) Notes on changing the settings in the cluster configuration
For the Management port, the administrator at the installation destination can use Hitachi File Services Manager to change the settings after the initial settings have been performed.
Note the following when setting the IP address, subnet mask (prefix length in case of IPv6), and default gateway:

(i) In case of IPv4, set IP addresses that do not begin with 0, 127, or 255.
Do not set IP addresses such as these: 0.xxx.xxx.xxx, 127.xxx.xxx.xxx, 255.xxx.xxx.xxx
By the IPv6 address of the Management port, the link local unicast address (fe80::/10) and the multicast address (ff00::/8) cannot be set.

(ii) In case of IPv4, set a correct subnet mask.
For example, 255.0.255.0 is not correct as a subnet mask because bit values are not contiguous.

(iii) For the IPv4 address, make sure that IP addresses and the default gateway host address you set do not become an address consisting of all 0s or 1s. For example, when the subnet mask is 255.255.255.0, you cannot set 192.168.0.0 or 192.168.0.255 as an IP address or the default gateway address.

(iv) Make sure that IP addresses and the default gateway address set to the same network segment (same address prefix in case of IPv6).
If you do not use a gateway address, you do not need to set it.
For example, when the subnet mask is 255.255.255.0, it is not correct that you set 192.168.0.16 and 192.168.1.1, whose network segments are different, as an IP address and the default gateway address.

(v) In the IPv4 address setting, make sure that the Management ports and BMC ports belong to the same network segment in the BMC and Management SW connection configuration.
Set the IP address for the network segment of Management port, BMC port, Private Maintenance port, Heartbeat port, and Reset port to prevent from the duplication in each other.
In the BMC direct connection configuration, set the IP addresses of BMC port and Reset port to be in the same network segment. And also set the IP addresses of BMC port and Reset port, Management port, Private Maintenance port, and Heartbeat port to be in the different network segment.

(vi) When a LAN device is connected to the Management port as an extension via a gateway, make sure that the network segment (same address prefix in case of IPv6) of the device is different from the network segment of the Private Maintenance port. If these network segments are the same, correct communication is impossible because of contention. You can also avoid the contention by using a command to change the IP address of the Private Maintenance port to an address that does not belong to the network segment of the LAN device connected via the gateway.

(vii) When the disk array subsystem is AMS2000 series, MSS, or HUS100 series, set the IP address of the same network segment of AMS2000 series, MSS, or HUS100 series maintenance port to the IPv4 address of private maintenance port.
In case of setting the IPv6 address, set the link local unicast address (the address within the range from fe80::1:0/64 to fe80::1:ff/64 and not matching the maintenance port) set in the maintenance port of AMS2000 series, MSS, or HUS100 series.
When the disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00 or HUS VM, set the IP address of private maintenance port that is different from the network segment of management port, BMC port, heartbeat port and data port.

Copyright © 2010, 2016, Hitachi, Ltd.

(a-2) Notes on changing the settings in the single node configuration
Note the following when setting the IP address, subnet mask, and default gateway:

(i) In case of IPv4, set IP addresses that do not begin with 0, 127, or 255.
Do not set IP addresses such as these: 0.xxx.xxx.xxx, 127.xxx.xxx.xxx, 255.xxx.xxx.xxx
By the IPv6 address of the Management port, the link local unicast address (fe80::/10) and the multicast address (ff00::/8) cannot be set.

(ii) In case of IPv4, set a correct subnet mask.
For example, 255.0.255.0 is not correct as a subnet mask because bit values are not contiguous.

(iii) For the IPv4 address, make sure that IP addresses and the default gateway host address you set do not become an address consisting of all 0s or 1s. For example, when the subnet mask is 255.255.255.0, you cannot set 192.168.0.0 or 192.168.0.255 as an IP address or the default gateway address.

(iv) In the IPv4 address setting, make sure that the Private Maintenance ports and BMC ports belong to the same network segment. Set the IP address for the network segment of Private Maintenance port, BMC port, Management port, and Data port to prevent the duplication in each other.

(v) When a LAN device is connected to the Management port as an extension via a gateway, make sure that the network segment (same address prefix in case of IPv6) of the device is different from the network segment of the Private Maintenance port. If these network segments are the same, correct communication is impossible because of contention. You can also avoid the contention by using a command to change the IP address of the Private Maintenance port to an address that does not belong to the network segment of the LAN device connected via the gateway.

(vi) In the Configuration using trunk 2 Data ports, the Management port is not be used for user daily operation. But in the case of performing system LU recovery, the Management port must be connected temporarily when newly installation will be performed to a vacant port of front-end LAN. Therefore, system administrator must keep 1 vacant port of front-end LAN to be connected the Management port.
When the disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00 or HUS VM, set the IP address of private maintenance port that is different from the network segment of management port, BMC port and data port.

Copyright © 2010, 2016, Hitachi, Ltd.

(b) Negotiation settings
Set the LAN interface negotiation.

(b-1) Initial settings

Table 5.1-2 Initial Value of Negotiation

Setting Item	Negotiation
Private Maintenance port	Automatic negotiation (10M/100M/1000M, half duplex/full duplex)
Heartbeat port	[100M/ full duplex] fixed
Management port	Automatic negotiation (10M/100M/1000M, half duplex/full duplex)
BMC port	Automatic negotiation (10M/100M, half duplex/full duplex)
Data port	No value is specified because interface information has not been assigned. The default setting when interface information has been assigned is automatic negotiation (10M/100M/1000M, half duplex/full duplex).
Reset port (pm1)	Automatic negotiation (10M/100M/1000M, half duplex/full duplex) *: This is used only in the BMC direct connection configuration.

(b-2) Notes on changing the settings
Make sure that the negotiation settings of a port and the device to be connected to the port are the same.
If the negotiation settings of connected devices are different, communication throughput may be deteriorated or communication may be impossible.

(c) MTU settings
Set the packet transmission size (Max Transfer Unit).

(c-1) Initial settings

Table 5.1-3 Initial Value of MTU

Setting Item	MTU
Private Maintenance port	1500 (fixed)
Heartbeat port	
Management port	
BMC port	
Reset port (pm1)	1500 (fixed) *: This is used only in the BMC direct connection configuration.
Data port	1500 (the default value to be used when setting interface information for data port.)

(c-2) Notes on changing the settings
(i) Make sure that the MTU settings of a port and the device connected to the port are the same.
If the MTU settings of connected devices are different, communication may be impossible.

Copyright © 2010, 2012, Hitachi, Ltd.

(d) Setting items in case of using the customer owned IP-SW
For IP-SW to be used for the management LAN, IP-SW provided by a customer may be used.
In this case, a maintenance personnel does not have to set IP-SW. However, the information regarding the customer IP-SW is shows below for reference.

- Customer provided IP-SW should be L2 switch (IEEE standard: IP-SW possessing IEEE 802.3 CSMA/CD, IEEE 802.3u Fast Ethernet).
- IP-SW provided by a customer has the two cases. One is the IP-SW provided solely for the management LAN and the other case is the IP-SW provided as the management VLAN of the separate segment in the common IP-SW with data LAN and so on.
- Depending on the LAN connection configuration in the customer environment, two cases may be available, One is the case that only the management port connects to IP-SW used for the management LAN, and the other case is that the management port and BMC port connect to IP-SW used for the management LAN.
- Interface requirements will be varied for each connection port.

Table 5.1-4 Interface Requirements of IP-SW Provided by Customer

Setting Item	Interface Requirement
Connection destination port of management port	Auto negotiation 100M: half-duplex/full-duplex 1000M: full-duplex
Connection destination port of BMC port	Auto negotiation 100M: half-duplex/full-duplex

Copyright © 2013, Hitachi, Ltd.

5.2 LAN Interface Security

(1) About the protocols used for Hitachi Data Ingestor in the cluster configuration
The following services are running to provide various types of services in Hitachi Data Ingestor.

Table 5.2-1 Ports Used by a node (1/2)

Port number	Protocol	Service name	Description
20	tcp	ftp	ftp-data port
21	tcp	ftp	Used for ftp
22	tcp	ssh	Used for ssh
22	tcp	sshd	Used for sftp. Also used as a data port.
53	udp	DNS	Used for DNS
69	udp	tftp	Used for tftp (It is used for OS version 4.2.0-XX or later)
88	udp/tcp	kdc	Used for user authentication in an Active Directory environment
111	udp/tcp	portmap	Used to manage the port numbers used by NFS-related services, and respond to inquiry from clients about port numbers
123	udp	ntp	Used for NTP
137	udp	NetBIOS Name Service	Used for the CIFS service via NetBIOS over TCP/IP
138	udp	NetBIOS Datagram Service	
139	tcp	NetBIOS Session Service	
161	udp	SNMP	Used for SNMP
162	udp	SNMP trap	Used for SNMP
199	tcp	SNMP Unix Multiplexer	For SNMP compatibility
389	tcp	LDAP	Used for the following two services: • User mapping using external LDAP • LDAP authentication Note: If a port number other than the default port number (389) is used, the port number can be specified from Hitachi File Services Manager.
389	udp	connectionless ldap	Used to check whether the DC server is alive or acquire DC information
443	tcp	https	Used for connection between the management server and the management console, communication with HCP, and communication with Hi-Track
445	tcp	Direct Hosting of SMB	Used for the CIFS service via Direct Hosting of SMB
464	udp/tcp	kpasswd	Used to join in a domain or change the user password in an Active Directory environment

Copyright © 2010, 2016, Hitachi, Ltd.

Table 5.2-1 Ports Used by a node (2/2)

Port number	Protocol	Service name	Description
514	udp	syslog	Used when SYSLOG is sent to other server.
750	tcp	kerberos4	Used for user authentication in an Active Directory environment
600 to 1023	tcp	NIS	Used for NIS
600 to 1023 (29998)	udp/tcp	rpc.rquotd	Used to retrieve Quote information from NFS client at the time of the NFS port dynamic allocation (default). A value ( ) is used in the OS version 4.2.0-XX or later when NFS port is fixed.
2049	udp/tcp	nfsd	Used for file shares by NFS
4045	udp/tcp	rpc.lockd	Used for region locks on file shares by NFS
8005	tcp	tomcat	Used for Tomcat shutdown Do not use in the OS version 6.1.0-XX or later.
8006	tcp	tomcat	Used for Tomcat shutdown Do not use in the OS version 6.1.0-XX or later.
8443	tcp	tomcat	Used for communication with Tomcat by HTTPS Do not use in the OS version 6.1.0-XX or later.
8444	tcp	tomcat	Used for communication with Tomcat by HTTPS Do not use in the OS version 6.1.0-XX or later.
9090	tcp	Management API	Receiving port for Management API
9090	tcp	HCP	Used for MAPI access to HCP
10000	tcp	ndmp	Used for NDMP
15000 to 15039, 19012, 19032	udp/tcp	Data Management	Used for Migration management port
20265	tcp	—	For maintenance, Program product installation, etc.
20266	tcp	—	
20287	udp	FailSafe	Used for communication with the remote node in a cluster configuration
20288	udp	FailSafe	Used for communication with the remote node in a cluster configuration
20289	udp	FailSafe	Used for communication with the remote node in a cluster configuration
20331	udp	—	Used by Shadow Image and True Copy
20332	udp	—	
30020 to 30499	udp	—	
31032 to 31254	udp	—	
31532 to 31754	udp	—	
22550	tcp	hfrrdmn	Used for HFRR (default port number)
21000 to 22499	tcp	—	Used for communication inside the FailSafe node
32768 to 61000 (20048)	udp/tcp	rpc.mountd	Used for the NFS mount request processing shared by NFS at the time of the NFS port dynamic allocation (default). (Port is not used in case of NFSv4) A value ( ) is used in the OS version 4.2.0-XX or later when NFS port is fixed.
32768 to 61000 (29997)	udp/tcp	rpc.statd	Used for the file lock recovery processing of the file shared by NFS at the time of the NFS port dynamic allocation (default). (Port is not used in case of NFSv4) A value ( ) is used in the OS version 4.2.0-XX or later when NFS port is fixed.

Copyright © 2010, 2016, Hitachi, Ltd.

Table 5.2-2 Ports Used by the Management Server (Hitachi File Services Manager)

Port number	Protocol	Service name	Description
443	tcp	https	Used to access the GUI
2000	tcp	SNM API	Used for changing LU settings
20265	tcp	Manager Agent	Used for authentication by using the account/password generated by the temporary-account login function during access to the GUI
22015	tcp	HBase 64	Used to access HBase 64 Storage Mgmt Web Service that does not support SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22016	tcp	HBase 64	Used to access HBase 64 Storage Mgmt Web Service that supports SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22017	tcp	HBase 64	Used to access the HBase 64 Storage Mgmt Common Service via AJP connection using the HBase 64 Storage Mgmt Web Service. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22018	udp	HBase 64	Used for HBase 64 Storage Mgmt Common Service to receive a termination request. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22032	udp	HBase 64	Used to access HiRDB. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22131	tcp	HBase 64	Used for internal communication of HFSM software component (naming service). This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22130, 22132, 22133	tcp	HBase 64	Used for internal communication of HFSM software component (Web service). This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
23015	tcp	HBase	Used to access HBase Storage Mgmt Web Service that does not support SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.
23016	tcp	HBase	Used to access HBase Storage Mgmt Web Service that supports SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.
23017	tcp	HBase	Used to access the HBase Storage Mgmt Common Service via AJP connection using the HBase Storage Mgmt Web Service. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.
23018	udp	HBase	Used for HBase Storage Mgmt Common Service to receive a termination request. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.
23032	udp	HBase	Used to access HiRDB. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.
45001 to 49000	tcp	HBase	Loop back port used for communication between HFSM software components (Hbase and HiRDB). This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later

Table 5.2-3 Ports Used by the Management Console (Web browser)

Port number	Protocol	Service name	Description
443	tcp	https	Used to access the GUI
22015	tcp	HBase 64	Used to access HBase 64 Storage Mgmt Web Service that does not support SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
22016	tcp	HBase 64	Used to access HBase 64 Storage Mgmt Web Service that supports SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.1.2-XX or earlier.
23015	tcp	HBase	Used to access HBase Storage Mgmt Web Service that does not support SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.
23016	tcp	HBase	Used to access HBase Storage Mgmt Web Service that supports SSL/TLS. This port do not use in the Hitachi File Services Manager version 6.2.0-XX or later.

Copyright © 2010, 2017, Hitachi, Ltd.

(2) About the protocols used for Hitachi Data Ingestor in the single node configuration
The following services are running to provide various types of services in Hitachi Data Ingestor.

Table 5.2-4 Ports Used by a node (1/2)

Port number	Protocol	Service name	Description
20	tcp	ftp	ftp-data port
21	tcp	ftp	Used for ftp
22	tcp	ssh	Used for ssh
22	tcp	sshd	Used for sftp. Also used as a data port.
53	udp	DNS	Used for DNS
69	udp	tftp	Used for tftp (It is used for OS version 4.2.0-XX or later)
88	udp/tcp	kdc	Used for user authentication in an Active Directory environment
111	udp/tcp	portmap	Used to manage the port numbers used by NFS-related services, and respond to inquiry from clients about port numbers
123	udp	ntp	Used for NTP
137	udp	NetBIOS Name Service	Used for the CIFS service via NetBIOS over TCP/IP
138	udp	NetBIOS Datagram Service	
139	tcp	NetBIOS Session Service	
161	udp	SNMP	Used for SNMP
162	udp	SNMP trap	Used for SNMP
199	tcp	SNMP Unix Multiplexer	For SNMP compatibility
389	tcp	LDAP	Used for the following two services: • User mapping using external LDAP • LDAP authentication
389	udp	connectionless ldap	Used to check whether the DC server is alive or acquire DC information
443	tcp	https	Used for connection between the management server and the management console, communication with HCP, and communication with Hi-Track
445	tcp	Direct Hosting of SMB	Used for the CIFS service via Direct Hosting of SMB
464	udp/tcp	kpasswd	Used to join in a domain or change the user password in an Active Directory environment
514	udp	syslog	Used when SYSLOG is sent to other server.
750	tcp	kerberos4	Used for user authentication in an Active Directory environment
600 to 1023	tcp	NIS	Used for NIS
600 to 1023 (29998)	udp/tcp	rpc.rquotd	Used to retrieve Quote information from NFS client at the time of the NFS port dynamic allocation (default). A value ( ) is used in the OS version 4.2.0-XX or later when NFS port is fixed.
2049	udp/tcp	nfsd	Used for file shares by NFS
4045	udp/tcp	lockd	Used for region locks on file shares by NFS
8005	tcp	tomcat	Used for Tomcat shutdown Do not use in the OS version 6.1.0-XX or later.
8443	tcp	tomcat	Used for communication with Tomcat by HTTPS Do not use in the OS version 6.1.0-XX or later.
9090	tcp	HCP	Used for MAPI access to HCP
9090	tcp	Management API	Receiving port for Management API
10000	tcp	ndmp	Used for NDMP

Copyright © 2010, 2016, Hitachi, Ltd.

Table 5.2-4 Ports Used by a node (2/2)

Port number	Protocol	Service name	Description
15000 to 15019, 19012	udp/tcp	Data Management	Used for Migration management
20265	tcp	—	For maintenance, Program product installation, etc.
22550	tcp	hfrrdmn	Used for HFRR (default port number)
32768 to 61000 (20048)	udp/tcp	rpc.mountd	Used for the NFS mount request processing shared by NFS at the time of the NFS port dynamic allocation (default). (Port is not used in case of NFSv4) A value ( ) is used in the OS version 4.2.0-XX or later when NFS port is fixed.
32768 to 61000 (29997)	udp/tcp	rpc.statd	Used for the file lock recovery processing of the file shared by NFS at the time of the NFS port dynamic allocation (default). (Port is not used in case of NFSv4) A value ( ) is used in the OS version 4.2.0-XX or later when NFS port is fixed.

Table 5.2-5 Ports Used by the Management Console (Web browser)

Port number	Protocol	Service name	Description
443	tcp	https	Used to access the GUI
20265	tcp	Manager Agent	Used for authentication by using the account/password generated by the temporary-account login function during access to the GUI

Copyright © 2010, 2016, Hitachi, Ltd.